European Commission

Project no. 732027

VIRT-EU

Values and ethics in Innovation for Responsible Technology in EUrope

Horizon 2020

ICT-35-2016

Enabling responsible ICT-related research and innovation

Deliverable 4.3

Second Report: Report to the internal members of the consortium on the PESIA methodology and initial guidelines

Due date: 31 December 2018

Actual submission date: 31 December 2018

Number of pages: 85

Lead beneficiary: POLITO

Author(s): Dr Maria Samantha Esposito, Prof Alessandro Mantelero, Prof Marcella Sarale, Dr ShairaThobani (Politecnico di Torino)* and Dr Selena Nemorin (LSE)

Actual submission date: 31 December 2018

Project Consortium

Beneficiary no.	Beneficiary name	Short name
1 (Coordinator)	IT University of Copenhagen	ITU
2	London School of Economics	LSE
3	Uppsala Universitet	UU
4	Politecnico Di Torino	POLITO
5	Copenhagen Institute of Interaction Design	CIID
6	Open Rights Group	ORG

Dissemination Level

PU	Public	**X**
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Dissemination Type

R	Document, report	**X**
DEM	Demonstrator, pilot, prototype	
DEC	Websites, patent filling, videos, etc.	
O	Other	
ETHICS	Ethics requirement	

* The authors are grateful to Laura Greco (research fellow at Politecnico di Torino) for the valuable contribution provided to this report in the analysis of PIA models and in drafting Section I.2.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the

Executive Summary

In the previous deliverable on the limits of GDPR (Deliverable 4.1. First report. Limits of GDPR and innovation opportunities) we discussed the approach adopted by the new General Data Protection Regulation[1] (hereinafter GDPR) and its adequacy in addressing the new challenges of Big Data, which represent the core of many IoT applications and related business models.

The first report pointed out several limitations affecting the existing regulatory framework which mainly concern the two following areas: (1) the relationship between risk assessment and data processing purposes; (2) the adoption of risk-assessment procedures which adequately consider the ethical and social impacts of data use.

These difficulties in addressing today's data-driven scenario confirmed the need to go beyond the existing models of data protection impact assessment and to adopt a more complex process of multiple-impact assessment. The latter should take into account both the individual and collective risks related to the use of data and, to this extent, also assess the potential interplay with societal issues.

Against this background, this deliverable (Deliverable 4.3. Second Report: This report to the internal members of the consortium describe the PESIA methodology and provides some initial guidelines) aims to outline the Privacy, Ethical and Social Impact Assessment (PESIA) model. This is one of the main goals of the Virt-EU project and a potential operative answer to the mentioned shortcomings.

To achieve this result, the following sections address two main research questions: which model should be adopted to design the PESIA? Which values should underpin this model?

On the basis of the answers to these questions, the deliverable provides to the members of the consortium a description of the PESIA methodology and some initial guidelines on the development of this model. More specifically, the contents of this deliverable concern the first part of the tasks described in T4.3 (Providing general and sector-specific guidelines for PESIA, M15-M27) and in T4.4 (Providing general and sector-specific instruments, M18-M27).

The findings discussed in this deliverable are the result of the merge of two different research approaches, combining the outcomes of the legal inquiry (carried out by POLITO) with the outcomes of the ethnological analysis (carried out by LSE and ITU). In this sense, the PESIA is the concrete result of a significant effort in terms of multi-disciplinary analysis and its development has fostered the cooperation between the different partners of the project.

Regarding the design of the model, the PESIA is based on the previous experiences of the Privacy Impact Assessment (PIA) and Data Protection Impact Assessment

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation.

(DPIA) schemes. For this reason, the second and the third sections of Part I of this deliverable deal with the different PIA/DPIA models adopted by several Data Protection Authorities within the European Union and in third countries. This overview of these schemes has provided useful guidelines to design the PESIA architecture.

From a methodological perspective, the main challenge in developing the PESIA model concerns the definition of the legal and societal (i.e. ethical and social) values that should underpin this model. To address this challenge, Section I.4 carries out an extensive analysis of the jurisprudence of the European Court of Human Rights and European Court of Justice, as well as of the jurisprudence of the national Data Protection Authorities of several EU countries. Similarly, from an ethnographic perspective, the last section of Part I (Section I.5) summarises the initial results of the analysis concerning the ethical and social values that are taken in to account by IoT developers and their communities in the design of their products and services.

In a scenario characterised by different sources of values, resulting from the legal and ethnological analyses, it is necessary to outline a common framework which can provide as suitable baseline for the PESIA. This goal has been achieved in the Second Part of this deliverable, mapping the identified values and their connections (Section II.2).

Finally, the last section of the deliverable (Section II.3) aims to transpose this map of values underpinning the PESIA in an efficient model which can be easily adopted by developers. To this end, this section provides some initial guidelines on the development of the PESIA model with a set of questions which extensively cover the privacy-focused section of the PESIA. Some indications and an initial set of materials (cases and questions) for the development of the sections concerning ethical and social values are also provided. According to the development of the research activities described in Tasks 4.3, 4.4 and 5.2, this last part of the deliverable will be further elaborated in the following months through the interaction with the communities of IoT developers. This will make it possible to better embed the viewpoints and the values of these communities in the PESIA model.

Part I – The values and methodology in PESIA development

I.1. Introduction

This First Part of the deliverable addresses two main research questions: which model should be adopted to design the PESIA? Which values should underpin this model?

Regarding the design of the assessment model, the PESIA is based on the previous experiences of the Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) schemes. This is due to two main reasons. First, PIA and DPIA models provide useful reference points, since these schemes are adopted in many countries. Second, the continuity with the impact assessment models generally used in the field of data protection can facilitate the adoption of the PESIA by IoT developers.

For these reasons, the PESIA model can be considered and described as an improvement of the exiting best practices in the field of impact assessment concerning the use of data. In this light, the second section of this deliverable deals with the different PIA models provided by several Data Protection Authorities within the European Union and in third countries. This analysis has made it possible to outline the main stages of the PIA models and to understand how to address both privacy issues and the emerging social and ethical issues. In the same vein, the structure of the DPIA (GDPR, Article 35) has been analysed, pointing out its main requirements.

This overview of the different PIA/DPIA schemes has provided useful guidelines to design the PESIA architecture. This architecture follows the PIA/DPIA structure, which is based on a list of questions. Nevertheless, unlike the PIA/DPIA schemes, the PESIA is not mainly focused on privacy issues, but is divided into three different thematic sections concerning privacy/data protection, ethical and social issues, respectively.

Regarding the first of these sections, the analysis of the existing models has made it possible to create a common framework for privacy assessment. This can contribute to the harmonisation of the GDPR-based assessment practices, which represents a key issue in today's regulatory debate in Europe.

With regard to the two sections focused on ethical and social issues, the main challenge concerns the selection of the societal values that should underpin these sections. To address this challenge, two empirical analyses have been carried out, focused on the legal and ethnographic domains.

The most extensive inquiry concerns the legal realm, since in this context ethical and social values are not explicitly mentioned or discussed in the decisions adopted by courts and data protection authorities. For this reason, the research required a significant effort in identifying these values in hundreds of cases decided by the European Court of Human Rights, the European Court of Justice and the data

protection authorities of seven different EU countries, as well as in the documents adopted by the Article 29 Data Protection Working Party. Through the analysis of more than nine hundred documents, it was possible to identify the main values used by courts and data protection authorities in their reasoning. This result provided a strong empirical evidence to design the PESIA sections on ethical and social impact.

The outcome of the legal analysis enriched by the results of the ethnographic analysis made it possible to draft a map of values which is the backbone of the PESIA sections on societal impacts. Moreover, the interplay between the legal and the ethnographic research and the achieved outcomes show how the core values identified in these two realms are largely the same, proving the internal coherence of the PESIA model.

I.2.1 The Privacy Impact Assessment Models (PIAs)

A Privacy Impact Assessment (hereinafter "PIA") is a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts[2]. In other words, the PIA process aims at examining the broad privacy implications of projects involving information with the final goal of identifying the risky areas of the project and, consequently, trying to find out ways to avoid or mitigate these risks.

PIAs have been more and more used during the 1990s and the industrial development, until our days where the risk governance and a strong privacy architecture have become essential for every organization. This trend has been confirmed with the introduction of the new regulation on data protection, the Reg. (EU) 2016/679, which provides for a similar analysis (but narrower and limited to the mere aspect of data protection) called Data Protection Impact Assessment.

There is no general model of PIAs. Sometimes countries have developed their own model and, other times, countries do not even have one. This fact is due to two main factors: on one hand, the lack of culture of privacy and the trend to a massive and unaware dissemination of information; on the other hand, the disregard about the impact that a project involving information could have upon our rights, our intimate sphere and, in general, our existence.

For these reasons, only few European countries have elaborated a PIA model so far and, even if these countries belong to different law systems, their PIA models result to be very similar as contents and structure.

This part of the project aimed at making a cross-analysis in relation to the methodology, the procedures and the core elements of a PIA by comparing the PIA models of some main European countries. The purpose was to detect the

[2] This definition is outlined in the final Deliverable n. 3 developed in the context of PIAF (*Privacy Impact Assessment Framework for data protection and privacy rights*), a European Commission co-founded project that aims to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy ad to the processing of personal data. The mentioned deliverable is available at the following link http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

commonalities among the models and so to identify a structure which could be taken as an example within the creation of a more complex model of PIA which takes account of fundamental rights and ethical and social values, as well.

The analysed European models of PIA are:

- Information Commissioner's Office, "Conducting privacy impact assessments Code of practice", February 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf;
- Agencia Española de Protección de Datos for Spain, "Guìa para la Evaluación de Impacto en la Protección de Datos Personales (EIPD)", 2014, https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf;
- Commission nationale de l'informatique et des libertés, "PIA Methodology", 2018, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf;
- Autoritat Catalana de Protecció de Dades for Catalunya, "Avaluació d'impacte relativa a la protecció de dades", 2018, http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-AIPD-APDCAT.pdf;
- Health Information and Quality Authority, "Guidance on Privacy Impact Assessment in health and social care", 2017, https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf.

The PIA models are mainly elaborated by the data protection supervisory authority of each country or region, precisely - in the cases considered in this analysis - the Information Commissioner's Office for the United Kingdom, the Commission nationale de l'informatique et des libertés (CNIL) for France, the Agencia Española de Protección de Datos for Spain, the Autoritat Catalana de Protecció de Dades for Catalunya. Instead, in Ireland the Health Information and Quality Authority[3] has been charged of the development of a PIA model for the health sector.

[3] The HIQA is the Irish independent Authority which has been established to drive continuous improvement in Ireland's health and social care services. The Authority's mandate extends across the quality and safety of the public, private (within its social care function) and voluntary sectors. Reporting directly to the Minister for Health and Children, the Health Information and Quality Authority has statutory responsibility for setting standards for Health and Social Services, Social Services Inspectorate, monitoring Healthcare Quality, Health Technology Assessment and Health Information. This latter includes the right to privacy, confidentiality and security of patients' personal health information.

I.2.2 The PIA concept and its main elements

The PIA is meant as an "on-going process", which shall be conducted for the time of the whole life-cycle of the project and even after it has been implemented, as new issues might arise following to the project's development[4]. But PIAs are also meant as a tool of the risk management[5], since organisations have accordingly understood that privacy is a strategic variable and assumes a relevant role in the success of a project or a product. This new concept comes from the knowledge that a lack of compliance and data breaches are negative factors: individuals' privacy being compromised would result in bad publicity and loss of public trust, which could lead to the rejection of an initiative by the public. Therefore, PIAs should not be simply seen as a compliance check, but as part of a project or risk management procedure in order to cover the sectorial specific angle of privacy.

- **Compulsory or optional assessment**

The PIA is not always a mandatory measure provided by law. In most cases, it is a recommended and voluntary assessment which can help organizations and, in general, controllers to respect the accountability principle showing their compliance with privacy principles and law[6].

- **Who could/should carry out a PIA**

Not all the analysed PIA models are direct to every subject and every organization. While the English, the French and the Spanish guides refer to any organization of the private and public sector which processes personal data, the Irish Guidance exclusively addresses healthcare providers who should assist "to identify potential risks around the collection and use of personal health information as this information is categorised as being sensitive" (p. 7).

[4] See, the abovementioned French Guide (p. 3).

[5] See, on the issue the English Guide, p. 3, 23 and the Annex V, which is completely dedicated to the integration of PIAs with project and risk management of organizations; the Irish Guide, p. 20; the French Guide, p. 2; the Spanish Guide, p. 15.

[6] The ICO clearly states that "conducting a PIA is not a requirement, but undertaking one will help to ensure that a new project is compliant. Whilst a PIA is not a legal requirement, the ICO may often ask an organisation whether they have carried out a PIA" (p. 8). The English Authority offers some examples of project which might require a PIA (pp. 9-10). Also the Spanish Data Protection Authority acknowledges that there is no formal obligation to conduct a PIA, but equally it asserts several benefits for the organizations which would carry out a PIA (p. 5), making an exemplifying list of cases where a PIA should be carried out (pp. 13-14). The CNIL, as well, considers the PIA as a discretionary measure which sometimes the law could provide for mandatory cases, but it does not point them out. The Catalonian guide follows the GDPR's provisions concerning the Data Protection Impact Assessment, therefore it provides only some specific cases where the DPIA is mandatory and, in particular, when the processing "is likely to result in a high risk to the rights and freedoms of natural persons". It is not clear whether conducting a PIA is mandatory or discretionary under the Irish Guidance, but the terminology used ("should", "can be", "are useful") lets suppose that there is no legal obligation to carry out a PIA. However, the importance and the fundamental role of the PIA is very much stressed ("PIAs form a fundamental part of information governance in assuring that patients' rights to privacy and confidentiality are appropriately protected", "PIAs are used across all sectors but are particularly useful for healthcare providers in assisting to identify potential risks", and so on).

- **When should be conduct a PIA**

A PIA should be carried out at the early stage of the project or of the initiative which implies a personal data processing. This best practice is shared by all the examined countries: conducting early a PIA allows to implement privacy principles and adapt the project before it is too late or too expensive to adjust the project in order to be compliant with law or privacy principles[7].

- **Team approach and responsibilities**

During the PIA every examined country reveals to adopt a "team approach" involving employees from different sectors of the same organization. This approach is very functional because it allows to acquire different perspectives resulting in a multidisciplinary set of information[8]. However, the responsibility of conducting the PIA does not necessarily lay with every member of the team, but only with the controller.

- **Templates**

All the examined countries make available templates and questionnaires to help organisations conducting their own PIA.

I.2.3 The main stages of a PIA

As above explained, PIA is considered as a process, thus it is structured with different stages. Every examined country has elaborated its own PIA procedure, but the stages are resulted to be common and can be resumed as below described.

- **Threshold of assessment / Identify the need of a PIA**

All the examined countries, except France[9], expressly provides for a first stage of identification of the need of a PIA. This stage consists of an initial assessment of a

[7] An early PIA implementation "will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly" and "identifying a problem early will generally require a simpler and less costly solution" (English Guide, p. 5 and 9). According to the Irish Guide, "a PIA is most beneficial when it is conducted in the early stages of a project – ideally at the planning stage" (p. 22). The PIA "should be implemented as soon as a new processing of personal data is designed. Implementing this approach at the outset makes it possible to determine the necessary and sufficient controls and thus to optimize costs" (French Guide, p. 3).

[8] "The PIA process should be undertaken by people with the appropriate expertise and knowledge of the project in question. As such, it should generally be undertaken by the project team" (Irish Guide, p. 22). "An effective PIA will include some involvement from various people in an organisation, who will each be able to identify different privacy risks and solutions" (English Guide, p. 10). The Spanish Guide considers important to create an interdisciplinary working group which will conducts the PIA and it dedicates to this theme the whole Chapter 3 (pp. 17-18).

[9] The French guide does not expressly provide for an initial stage concerning the decision of conducting a PIA, but it offers some examples of stakeholders, involved in creating or improving processing of personal data or products, for whom the PIA could be useful (p. 2).

project, to determine whether its potential privacy impact necessitates a PIA. A threshold assessment should be undertaken for every new project but also for proposals which intend to amend existing systems, processes or projects.

The threshold assessment can consist of a checklist of questions (like in the Irish and English guides) or an illustrative list of cases where a PIA is recommendable (like in the Spanish guide).

One that this threshold assessment is completed, the controller (or the project team) might decide to proceed or not with the PIA. In either case the completed threshold assessment should be approved by the project lead and senior management and documented.

- **Description of the project and information flows**

If the necessity of a PIA arises from the execution of the threshold assessment, the controller (or the project team) should proceed with the description of the project and the information flows. In particular, this stage aims at exploring the project's context and scope (with details about the controller, the person proposing the project, the overall aims of the project), information flows and security measures.

This stage is fundamental since it puts the basis of a thorough assessment of privacy risks which is only possible if an organisation fully understands how information is being used in a project.

All the examined countries provide for this stage but with different degree of detail. For example, in the Irish Guidance this stage includes also a review of the general privacy management of the organization, namely how the service provider manages the privacy of information within the organisation, exploring information governance issues such as data protection and confidentiality, education, training of staff and accountability for the handling of personal information[10]. The description of the project and the information flows is not an end in itself, but it is aimed at the risk identification.

Regarding to the Catalonian guide, a systematic description of the envisaged processing operations and the purposes of the processing is required, pursuant to Art. 35 of the GDPR. The Catalonian Authority specifies that this set of information should include details about the data sources and the means of processing (including automated or not means), a categorisation of the personal data, procedures for the data recording and storage, the identity or kind of people who can access to personal information, the use of technologies[11].

- **Identify and analyse the risks**

In this phase the controller, or the project team, should identify and analyse the privacy risks of the processing activities, which have been described in the previous stage. For this purpose, it is necessary to identify the relevant risk sources (which could regard human, technical or organizational factors), the likelihood of their occurrence and the degree of their impact on privacy and on involved subjects.

[10] See the Irish Guidance, pp. 29-33.
[11] See the Catalonian guide "Avaluació d'impacte relativa a la protecció de dades", pp. 36-44.

Actually, in this stage, from the controller's perspective, the risks to be taken into account are not only those which could affect privacy, data protection and data subjects, but also those risks which regard the organization itself, like regulatory action, fines for non-compliance with legislation, reputational damages and loss of public trust. Once risks have been identified and examined, it should be maintained a record of the identified risks.

Except the Irish Guidance which includes this stage in the previous one related to the description of project and information flows, all the examined countries provide for an autonomous and separate stage for the identification and analysis of risks[12].

- **Consultation**

This stage represents an important step in the PIA process since it allows the collection of opinions and views of different people (internal and external the organization) who might highlight privacy risks and solutions based on their own area of interest or expertise[13]. Even if we refer to this stage at this point of the analysis, organizations should not see it as a separate step: it can be useful to build consultation into all stages of the PIA process. This allows organisations to consult the right people at the right time and avoid having to spend more time and resources on a separate exercise.

- **Management of the risks**

Once risks have been identified and analysed, controller, or the project team, should evaluate which privacy solutions and actions could be taken to address those risks. It is important to remember that the aim of a PIA is not to completely eliminate the risk impact on privacy, but at least to mitigate it to an acceptable level while still allowing a useful project to be implemented. Indeed, it is still possible to have a residual or remaining risk, which cannot be mitigated: in this case, the controller, or the project team, should decide whether or not it is acceptable to continue with the project.

The available options for addressing each risk might result in the risk being eliminated, reduced or accepted, except for those risks related to the non-compliance with legislation which should be exclusively eliminated or avoided.

All the examined countries provide for this important stage, but with different levels of detail[14].

---

[12] See, p. 6 of the French Guide; pp. 21-26 of the Spanish Guide; pp. 58-61 of the Catalonian Guide; pp. 23-26 of the English Guide.

[13] See, pp. 23-24 of the Irish Guide; pp. 27-28 of the Spanish Guide; pp. 36-38 of the Catalonian Guide; pp. 16-19 of the English Guide. The French Guide does not expressly mention this stage or, in any case, this practice of involving stakeholders and subjects who can contribute to the PIA.

[14] The English Authority makes some examples of measures which organisations can take to reduce a privacy risk (e.g. deciding not to collect or store particular types of information; devising retention periods which only keep information for as long as necessary and planning secure destruction of information; see, p. 27-29). The Irish Guide and the Spanish Guide provide for a list of different solutions to address the risks as well (respectively, pp. 35-38 and pp. 30-44). The French guide does not provide for a specific management of risks, but an evaluation of the PIA consisting of a review of the preceding steps' results and the planned controls. If the controls are implemented and the risk are treated in an acceptable way, they might proceed to the formal validation of the PIA or to the preparation of an action plan in order to implement the planned controls. On the contrary, they should

- **The PIA report**

Although it is not a mandatory requirement, the production of a PIA report is a good practice since it sums up the proposed project, the steps that were undertaken as part of the PIA process and any subsequent recommendations. A completed PIA report should highlight and address all privacy risks associated with the project and the steps which have been taken to mitigate or avoid them.

This practice is provided by all the examined countries which describe in detail the report's contents, structure and format. According to the examined PIA models, the PIA report should contain the following information at least:

- A detailed description of the project including the objectives and justification for the project, the responsible team/subjects and their contact details
- An overview of the PIA process undertaken explaining the outcomes (possibly for each stage), with an emphasis on the scope and information flows of the project
- A description of the specific risks which have been identified, the solutions considered to mitigate or avoid these risks and a rationale for the decisions made
- Details of any consultation which took place with stakeholders (both internal and external the organization), users or the general public.

These are the main structure and contents which are commonly shared by the examined countries[15].

The publication of the report is not mandatory, but it is considered a good practice which can increase accountability and transparency and has the effect of inspire public confidence by allowing the public to understand how their information is used. The report may be disclosed in a complete way or in a summary version, if it contains sensitive information which it is not appropriate to disclose, such as information on security measures or intended product development[16].

- **PIA outcomes and review of the PIA**

Organisations need to make sure that the results of the PIA and the consequent agreed privacy solutions are integrated back into the project plan to be developed and implemented.

Besides, the PIA should be periodically reviewed, especially when the examined process is subject to significant alterations or development. In such cases,

---

propose additional controls and re-assess the level of each of the risks in view of the latter, so as to determine the residual risks (p. 7).

[15] Then, some PIA models provide for additional information such as a copy of the threshold assessment form and an outline of any remaining risks which could not be resolved together with a business case justifying why it has been decided to accept these risks and proceed with the project and the likely implications for the public or service users involved (Ireland). In other cases, a list of legal controls and risk-treatment controls is included in the PIA report (France). A law compliance check and the PIA team's recommendations are put in the report as well (Spain).

[16] See, pp. 40-41 of the Irish Guide; pp. 46-47 of the Spanish Guide; p. 31 of the English Guide; pp. 73-74 of the Catalonian Guide.

organisations need to evaluate if the PIA's outcomes and the privacy solutions adopted are still valid and efficient in the light of the changes.

The examined PIA models briefly describe this step, only stating the importance of the recommendations' implementation and the review as final stages of the PIA process[17].

I.2.4 The emerging social and ethical values in PIA models

In no PIA model, social and ethical values are explicitly mentioned, but it is possible to infer these values from the purposes and the structure of the elaborated PIA models.

Firstly, there is the need to consider the dual function of the PIA. From an organisation's perspective, the PIA is a risk management tool and helps organisations to identify risks and solutions through a prior evaluation. In this way, the PIA allows organisations to understand in a precautionary way which risks exist and to prevent their realization, so that they might avoid costs which they would have to bear in order to fix the damages coming from the materialisation of the risk.

However, the PIA – when it is conceived as a public report to disclose – has also another relevant and hidden function. By analysing the process and providing for the best privacy solutions, it represents an important tool for the affected people as well. Thanks to PIAs they are able to know how their information is used and which safeguards are put in place in order to protect their information. Therefore, here the protected values can be identified in the transparency and control of one's own information and the main means to ensure these values is the final report.

Lastly, it is not to be forgotten that another relevant purpose of making a PIA lays with the accountability principle, which postulates not only to be responsible for, but also to be able to demonstrate compliance with the law. The PIA facilitates this proof and, at the same time, increases the protection of data subjects.

As already noted, no values are specifically described in the examined PIA models; however, in some cases it is possible to observe some (usually vague) references to them.

The ICO's guide provides for some questions under Annex III which are aimed at identifying risks which the project will fail to comply with the DPA or other relevant legislation. Among these questions, it is asked if social needs are taken into account and, in case of positive response, if the assumed actions are proportionate to the social need. Besides, in the English guide the impact of operations regarding personal data is identified in relation not only to the physical safety of individuals or referring to other possible material impacts, but also regarding the moral sphere of people, like the distress caused.

In other cases, conducting a PIA could aim at ensuring equality of treatment, non-discrimination and individuals' dignity. Among the examples of processing which

[17] See, pp. 42-43 of the Irish Guide; pp. 48-49 of the Spanish Guide; p. 32 of the English Guide; pp. 75-77 of the Catalonian Guide.

shall require a PIA, the Spanish guide includes the case of processing which, evaluating personal aspects and profiles of individuals and their behaviours, could lead to different treatments or influence their dignity or personal integrity.

The French guide protects values as dignity and freedom of individuals[18] as well. Among the rules for estimating risks and their severity and likelihood, it includes the evaluation of moral impacts on individuals, meaning physical or emotional suffering, disfigurement or loss of amenity, which might lead to a negligible, limited, significant or maximum risk. Some examples of moral impact related to the level of risk which implies, are outlined below:

- The feeling of invasion of privacy without real or objective harm brings about a negligible risk;
- Minor but objective psychological ailments (defamation, reputation) or relationship problems with personal or professional acquaintances imply a limited risk;
- The feeling of invasion of privacy with irreversible damage, of violation of fundamental rights (e.g. discrimination, freedom of expression), cyberbullying or harassment cause significant risks;
- Long-term or permanent psychological ailments, criminal penalty or loss of family ties produce maximum risks[19].

I.2.5 Additional considerations and references to the new guides on GDPR

The analysis has examined the most relevant existing PIA models, but it is worth noting that other countries are trying to develop PIA guides as well.

For example, Belgium has drafted a project of recommendation on Data Protection Impact Assessment which has been recently approved. In this case, the recommendation is outlined on the GDPR and, specifically, on the obligation pursuant to Art. 35 (DPIA). Although this act mainly regards the DPIA and the risks whose existence leads to the necessity of a DPIA, it expressly mentions that these relevant risks may also concern other fundamental rights and freedoms than the sole data protection, such as freedom of speech, freedom of thought, freedom of conscience and religion, prohibition of discrimination and of movement[20].

---

[18] In particular, in the second document regarding the PIA called “Tools”, June 2015.
[19] The complete list of examples is available at pp. 13-15 of the French PIA guide “Tools”.
[20] The Belgian act reproduces the list of cases which the Working Party Group Art. 29 has elaborated in relation to the concept of “a processing which substantially affects data” in the context of a cross-border processing (see *Guidelines for identifying a controller or processor’s lead supervisory authority,* WP244 rev.01, as last revised and adopted on 5 April 2017). In order to correctly interpret this concept, the WP Group Art. 29 suggests considering the following factors, such as whether the processing (p. 4):
- causes, or is likely to cause, damage, loss or distress to individuals;
- has, or is likely to have, an actual effect in terms of limiting rights or denying an opportunity;
- affects, or is likely to affect individuals’ health, well-being or peace of mind;
- affects, or is likely to affect, individuals’ financial or economic status or circumstances;
- leaves individuals open to discrimination or unfair treatment;

Also the Netherlands[21] have released a guide describing what is a PIA, when it is necessary, who it concerns and which aspects are to be taken in account in order to fulfil a PIA. However, in this case, the PIA requirement addresses overall the national government which is obliged to consider the results of a PIA when developing new legislation. Besides, the NOREA (the professional organization of IT auditors) issued, in collaboration with the Dutch Data Protection Authority, a study report[22] which describes the stages of the PIA process, including a questionnaire and a list of success and failure factors in the implementation of PIA. This document is important because it is one of the few explicitly pointing out values which may be compromised by the infringement of the privacy of the data subject.

Germany[23] and Austria[24] have approved implementation bills of the GDPR as well, but they do not examine the DPIA, nor gives additional information or suggestions about this obligation. However, in relation to PIAs in the German context, it is worth noting that the Conference of the German Independent Data Protection Authorities of the Bund and the Länder has released a draft of the so called Standard Data Protection Model[25] which does not properly regard a PIA, but it provides a methodology for assessing the efficacy of data protection measures required by data protection regulations, especially taking into account the GDPR provisions. Although it does not describe a PIA process[26], it is interesting to note that the SDM is directed not only to controllers who are enabled through it to systematically plan, implement and continuously monitor the necessary functions and protection measures, but also to supervisory authorities enabling them to reach a transparent and plausible, reliable judgment on a procedure and its components.

- involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children;
- causes, or is likely to cause individuals to change their behaviour in a significant way; o has unlikely, unanticipated or unwanted consequences for individuals;
- creates embarrassment or other negative outcomes, including reputational damage; or
- involves the processing of a wide range of personal data.

[21] On the 9th December 2017 the Dutch Minister of Security and Justice published the draft "Implementation Act of the General Data Protection Regulation" (the "Implementation Act"). The draft has been recently sent to the Parliament for its approval. The whole process can be followed here: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34851.

[22] "Privacy Impact Assessment (PIA) Introductie, handreiking en vragenlijst", Vers. 1.2, last update on November 2015.

[23] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), vom 30. Juni 2017. The legislative text is available here: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1524067402355.

[24] Austria has officially published on July 31, 2017 the "Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)". The official text is here available: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig.

[25] "The Standard Data Protection Model. A concept for inspection and consultation on the basis of unified protection goals", V. 1.0 – Trial Version, 9-10 November 2016.

[26] The structure of the SDM is divided into several staged that aim at reaching the following goals: 1) transferring legal data protection requirements into a catalogue of protection goals, 2) structuring the procedures under consideration into the components data, IT-systems and processes, 3) incorporating the classification of data in three tiers of protection levels, 4) complementing these with considerations on the level of procedures and IT-systems and 5) providing a systematically derived catalogue of standardised data protection measures, which have been systematically derived from these principles.

On the basis of the current analysis, we can conclude that the analysed models do not help in the identification of ethical and social values, which seem not to be mentioned. However, cases, examples and references reveal that actually moral aspects have been taken in account in the elaboration of the models.

The result of this analysis shows that the above-identified structure of a general PIA process is suitable for the creation of a PESIA model. However, unlike a general PIA, the PESIA should be enriched of explicit mentions and references to ethical and social values which should represent leading factors and main grounds for the identification of potential risks deriving from a project involving personal information.

I.3.1 The Data Protection Impact Assessment Model (DPIA)

Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR) provides for a mandatory Data Protection Impact Assessment (DPIA). DPIA is not new in the regulatory framework, however GDPR dictates a specific discipline which was previously lacking.

DPIA can be seen in the broader context of a risk-based approach to data protection, which implies the adoption of strengthened measures the more the processing is deemed to be risky. The previous (and now repealed) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data also contained some provisions which reflect a risk-based approach.[27] Article 17, regarding the security of processing, imposed the adoption of security measures "appropriate to the risks represented by the processing and the nature of the data to be processed" and Article 20 provided for a prior checking to be carried out by the data protection supervisory authority in cases, determined by Member States, when the processing was "likely to present specific risks to the rights and freedoms of data subjects".

GDPR generalises the obligation to carry out a DPIA, introducing a specific procedure and specifying the criteria under which a DPIA is compulsory. This approach is also the result of the accountability principle adopted by GDPR, under which the controller shall "be able to demonstrate compliance" with data protection regulation (art. 5, para 2 GDPR). In this light, "DPIA is a process for building and demonstrating compliance".[28]

GDPR provides for different levels of assessment. A first one consists in the general duty to implement all the necessary measures in order to tackle the risks deriving from the processing. A second level consists in the DPIA, for which GDPR requires a specific procedure to be followed. Finally, on the third level there is the prior consultation with the supervisory authority on the adopted measures.

[27] Art. 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218, adopted on 30 May 2014, p. 2.
[28] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, adopted on 4 April 2017, revised and adopted on 4 October 2017, p. 4.

- **General risk analysis**

Article 24 GDPR provides that "[t]aking into account the nature, scope, context and purpose of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary". To be able to identify the measures to adopt, it is clear that the controller shall previously carry out an assessment of the impact of the processing on the rights and freedoms of data subjects and on the risks it entails.

Such provision is to be read in conjunction with Article 5 (1) GDPR, which lays down the principles relating to the processing of personal data, i.e. lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. The controller shall therefore adopt the measures necessary to comply with such principles, which need to ensure that the risks deriving from the processing are kept under control.

Such provision is also to be read in conjunction with Article 25 GDPR, regarding data protection by design and by default. Under the data protection by design principle, the technical and organisational measures to ensure compliance and to address risks shall be adopted *ex ante* "at the time of the determination of the means for processing and at the time of the processing itself". Such measures shall therefore be integrated in the technical means of the processing. Under the data protection by default principle, the necessary measures to ensure data minimisation and security shall be implemented by default, i.e. from the beginning of the processing, and not applied after the processing has already started.

- **Data protection impact assessment**

The measures adopted following the general risk analysis may already be sufficient to address the risks of the processing. However, if the risks are particularly high, the GDPR requires to carry out a more formalised data protection impact assessment. In particular, a DPIA is necessary "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons" (art. 35, para 1 GDPR.)

The GDPR (art. 35, para 3) offers some examples of circumstances that carry a high risk and therefore require a DPIA:

(a) "a systematic and extensive evaluation of personal aspects relating to natural persons which Is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1) [data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health, sex life or sexual orientation], or of persona data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale."

Finally, a DPIA is compulsory if the processing falls within the public list established by the supervisory authority (art. 35, para 4.)

On the contrary, a DPIA is not compulsory if[29]:

- The general risk analysis has revealed that the processing is not likely to result in a high risk to the rights and freedoms of data subjects;

- A DPIA has already been carried out for a very similar processing which presents the same risks as the processing in question;

- The processing is included on the list of processing operations which do not need a DPIA, which can be issued by national supervisory authorities (art. 35, para 5).

- **Prior consultation**

The DPIA shall identify the measures necessary to mitigate the risks posed by the processing. However, if the envisaged measures are not sufficient to tackle such risks, which remain high, the controller is compelled to consult the supervisory authority before starting the processing (art. 36 GDPR.)[30]

In the prior consultation process, the supervisory authority verifies the whole assessment carried out by the controller and, in particular, if the risks have been correctly assessed and if the measures to tackle such risks have been properly identified. If they have not, the supervisory authority shall identify the measure that the controller must adopt in order to mitigate the risks. However, it is also possible that the risks are too high to be addressed: in this case, the supervisory authority shall prohibit the processing.

In addition to this general obligation of prior consultation, Member States may require additional prior consultation or authorisation proceedings by the supervisory authority if the controller carries out the processing for the performance of a task of public interest, such as, for instance, social protection or public health.

I.3.2 Requirements for a DPIA

As mentioned, there are certain circumstances which trigger the obligation to carry out a formal DPIA. More precisely, it is mandatory to carry out a DPIA if the processing is "likely to result in a high risk to the rights and freedoms of natural persons". In order to verify if these circumstances are present, the controller shall

[29] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, pp. 12-13.

[30] The wording of art. 36 GDPR might be literally interpreted in the sense that the prior consultation is necessary in all cases in which the processing results in high risks. The prevalent interpretation is, however, that the prior consultation is necessary only if the residual risks (i.e. the risks that remain after the adoption of the measures envisaged by the DPIA) are high. In this sense see recital no. 84, under which "Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing." See also Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 18.

always carry out a previous risk assessment. Even if there is no formal procedure for the latter, it falls within the general duties of the controller to perform a general risk analysis in order to comply with the regulatory requirements and to verify whether a formal DPIA is needed. Such an analysis shall be reviewed regularly as risks may change over time.[31]

The risks to rights and freedoms of natural persons (which shall be evaluated according to their likelihood and severity) refer, in the first place, to the risks to data protection and privacy rights, the infringement of which could lead to physical, material or non-material damage. It is the case, for instance, where the processing may give rise to "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data […]" (Recital no. 75 GDPR.) Besides data protection and privacy rights, risks may also involve other fundamental rights, such as freedom of speech, freedom of thought, freedom of movement, right to liberty, conscience and religion.[32]

As mentioned, the GDPR offers some examples of cases in which there might be high risks to fundamental rights and freedoms: (a) when there is a systematic and extensive evaluation of personal aspects which is based on automated processing and which represents the basis to take decisions that significantly affect natural persons; (b) when the processing is carried out on a large scale and involves sensitive data; (c) when there is a systematic monitoring of a publicly accessible area on a large scale.

It is important to underline that these are mere examples and do not amount to an exhaustive list. This means, on the one hand, that there might be cases that fall outside this list but still require a DPIA; on the other hand, there might be cases, however exceptional, that fall within this list but do not require a DPIA. As an example of the latter, there might be some cases that are expressly excluded by the supervisory authority from the obligation to carry out the DPIA (art. 35, para. 5.)

In order to identify when a DPIA is compulsory, supervisory authorities can issue specific lists of processing operations that need it.[33] In any case, these lists, however useful for the implementation of the regulatory requirements, are to be considered as non-exhaustive. It is therefore important to identify certain criteria to help guiding controllers when assessing the need to carry out a formal DPIA. To such end, Article 29 Working Party has issued some specific guidelines,[34] which specify the following criteria:

[31] Under art. 35, para. 11 GDPR "Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations". See also Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 6.
[32] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 6.
[33] The lists adopted by the different national DPAs are available here: https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_it.
[34] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, pp. 9-11.

- ✓ "Evaluation or scoring, including profiling[35] and predicting, especially from '*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements*' (recitals 71 and 91)". Evaluation and scoring operations are considered risky in themselves, as they might deliver inaccurate predictions and, in any case, they represent the necessary preliminary step to carry out discriminatory practices. Moreover, profiling can "perpetuate existing stereotypes and social segregation."[36]
- ✓ "Automated-decision making with legal or similar significant effect:[37] processing that aims at taking decisions on data subjects producing '*legal effects concerning the natural person*' or which '*similarly significantly affects the natural person*' (Article 35(3)(a))". For the processing to pose a high risk to fundamental rights and freedoms it is not necessary that the decision-making processes be solely automated; however, the more the human involvement, the less the risks deriving from the processing. Risks are high if the automated decision-making has legal effects on the individual, i.e. if it affects his or her legal rights: this could be the case, for instance, it the data processing leads to the cancellation of a contract, to the denial of social benefits or of admission to a country, to the restriction of voting rights.[38] Risks are also high if the automated-decision making "similarly significantly affects" the individual. As specified by the Art. 29 Working Party, this means that "the decision must have the potential to significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals."[39] This is particularly the case when the decision regards the access to services or activities that are of great importance for the individual, such as health, banking or education services, or employment opportunities.[40]
- ✓ "Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or a "systematic monitoring of a publicly accessible area" (Article 35(3)(c))." In this case, risks may be high considering that individuals may not be aware of the processing

[35] Art. 4, no. 4 GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

[36] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/677*, WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, pp. 5-6.

[37] See art. 22, para 1 GDPR , which states the right of the data subject "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her." See also recital no. 71.

[38] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling*, p. 21.

[39] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling*, p. 21.

[40] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling*, p. 21-22. See also recital 71 GDPR, which gives as an example the "automatic refusal of an online credit application or e-recruiting practices without any human intervention."

and (especially if the monitoring regards a publicly accessible area) may not be able to avoid it.[41]

- ✓ "Sensitive data or data of a highly personal nature". Sensitive data include both the special categories of data as defined by art. 9 (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health, sex life or sexual orientation) and data relating to criminal convictions and offences (art. 10.) However, the notion of sensitive data is not limited to what is provided for by GDPR, but also includes other kinds of data which are closely related to fundamental rights: for instance, data "linked to household and private activities (such as electronic communications whose confidentiality should be protected)", data which could "impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement)", data whose violation "clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud)".
- ✓ "Data processed on a large scale". In order to evaluate what is to be considered as "large scale", the following circumstances should be taken into account: "a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity". As regards the latter requirement, Recital no. 91 GDPR specifies that the "large-scale" criterion should be evaluated "at regional, national or supranational level", further clarifying that is not to be considered on a large scale the processing carried out by single professionals, such as personal data from patients or clients processed by an individual physician or lawyer.
- ✓ "Matching or combining datasets". These operations may pose high risks to the data subjects with regard to their level of awareness and control over their data. This is especially the case if the combined datasets have been collected by different controllers or for different purposes, as the individual will not normally expect those data to be combined.
- ✓ "Data concerning vulnerable data subjects". This category includes both vulnerable sectors of the population (such as children, elders, patients, asylum seekers), and individuals who are in an imbalanced position with respect to the controller, such as employees. These subjects deserve a higher protection as they may not be completely aware of the processing nor able to understand its consequences, or may be in a position which makes them particularly vulnerable to the decisions taken by the other party.
- ✓ "Innovative use or applying new technological or organisational solutions" The occurrence of high risks is particularly relevant and should be very carefully assessed with regard to new technologies.[42] On the one hand, the novelty factor implies that the risks these technologies might give rise to are not yet renowned and explored. On the other, the evolution of technology may result

[41] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 9.
[42] See Recital no. 89 and Article 35, para 1 GDPR.

in higher levels of intrusiveness and pervasiveness. This specially applies to IoT applications, which "could have a significant impact on individuals' daily lives and privacy."

- ✓ "When the processing in itself 'prevents data subjects from exercising a right or using a service or a contract (Article 22 and recital 91)." Even if the processing is not automated, it could still pose high risks to individual rights and freedoms if it is used to take decisions concerning the access to services and the entering into contracts, especially if such services or contracts are of a significant importance to the individuals, such as bank loans.

I.3.3 How to carry out a DPIA

- **Who to involve**

First, it is important to identity who, among all those involved in the data processing operations, is responsible to carry out the DPIA. According to the GDPR, this obligation falls on the controller (i.e. the natural or legal person who determines the purposes and means of the processing), meaning that he shall ensure that the DPIA is carried out and remains accountable for it, while the DPIA may materially be conducted by someone else[43] and can even be outsourced.

The controller does not operate alone, but "shall seek the advice of the data protection officer, where designated" (Article 35(2)) and shall be assisted by the data processor (Article 28(3)(f)).

The data protection officer has the duty to provide advice on the DPIA and to monitor its performance (Article 39 (1)(c)) As recommended by the Art. 29 Data Protection Working Party, the controller should consult the data protection officer on "whether or not to carry out a DPIA; what methodology to follow when carrying out a DPIA; whether to carry out he DPIA in-house or whether to outsource it; what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR."[44]

The processor should also be involved: considered that the processor processes personal data on behalf of the controller, this figure can offer precious insight on the risks of the processing and ensure the effectiveness of the measures identified to mitigate risks.

When it is "appropriate", the controller shall also "seek the views of the data subjects" (Article 25 (9)) It is to be noted that, according to the interpretation given by the Art. 29 Data Protection Working Party, such a consultation seems to be compulsory, meaning that if the controller decides not to carry it out, the controller

[43] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 14.
[44] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243, adopted on 13 December 2016, p. 17.

shall document the reasons why.[45] Legitimate reasons not to consult the data subjects could be that such a consultation risks to jeopardise "the protection of commercial or public interests or the security of processing operations" (Article 35 (9)). This could be the case, for instance, if it compromises the confidentiality of business plans, or when it would result "disproportionate or impracticable".[46] How to conduct such a consultation should be assessed taking into account the specific context and feasibility: for instance, the controller could deliver a survey to staff representatives or to his future customers, or carry out a generic study.[47]

- **Stages of the DPIA**

As regards the methodology to adopt when carrying out the DPIA, the GDPR set out some minimum requirements (Article 35 (7)).

First, the DPIA shall contain "a systematic description of the envisaged processing operations and the purposes of the processing" and "an assessment of the necessity and proportionality of the processing operations in relation to the purposes" (Article 35 (7) (a) (b)) The first phase of the DPIA is therefore a preliminary one, which serves to establish the context against which the risks will then be evaluated. The DPIA should indeed take into account "the nature, scope, context and purposes of the processing and the sources of the risk" (Recital no. 90.)[48] The analysis of these aspects is also meant to help the controller implementing the minimisation principle, under which only the data which are strictly necessary to the envisaged purposes should be processed. It is clear the correct implementation of the minimisation principle constitutes, by itself, a measure to mitigate risk.

Secondly, the DPIA shall contain "an assessment of the risks to the rights and freedoms of data subjects" (Article 35 (7) (c)) At this stage, the controller should take into account all the criteria listed above which regard the risks to fundamental rights and freedoms and identify such risks, assessing them by their likelihood and severity.[49] The controller should also take into account which measures have already be taken to mitigate the risks, as, for instance, the compliance with approved codes of conduct (Article 35 (8)).

Finally, the assessment needs to provide for "the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation" (Article 35 (7) (d)). These measures shall operate *ex ante*, following the principles of privacy by design and privacy by default so that the measures are incorporated in

[45] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 15.
[46] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*,, p. 15.
[47] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*,, p. 15.
[48] According to the Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, Annex 2, the DPIA should list the nature, scope, context and purposes of the processing, the personal data which are collected, the recipients and the period for which the personal data will be stored, a functional description of the processing operations, the assets on which personal data rely (hardware, software, people, paper, networks…)
[49] The Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, Annex 2, seems to take into account security risks in particular, citing as potential risks "illegitimate access, undesired modification, and disappearance of data."

the processing itself. It is also important that the DPIA clearly states which are the tasks and responsibilities of each of the parties involved in the processing.

Once the DPIA is completed, the Art. 29 Data Protection Working Party suggests considering whether to publish it at least partially or in a summarised version.[50] Publication of the DPIA is not compulsory, however it would contribute to fostering trust in the controller's data processing operations and it would be a significant sign of transparency.

It is important to underline that the duty to carry on an assessment does not end when the DPIA is completed. It is, indeed, a continuous process. The controller "shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations" (Article 35 (11)). First, there shall be a continuous monitoring regarding the compliance of the measures envisaged by the DPIA. Secondly, as risks may change over time depending not only on changes in the processing operations but also on the evolution of the broader social and technological context, the controller shall periodically assess if the risks have changed and if the envisaged measures are still sufficient to tackle them.

- **Single DPIA for multiple processing operations**

It is finally important to underline that if there are sets of different processing operations "similar in terms of nature, scope, context, purpose, and risks",[51] then a single DPIA can suffice. This can be the case not only when the different processing operations are carried out by the same controller, but also if they are performed by different controllers.

As explicitly stated by the GDPR, "[a] single assessment may address a set of similar processing operations that present similar high risks" (Article 35 (1)) This may also seem the rationale behind the provision that rules out the need of a DPIA in case the processing has a legal basis and a DPIA has already been carried out (Article 35 (10)) In more general terms, "[t]here are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity" (Recital no. 92).

This may be especially relevant when the DPIA regards the processing operations that arise from the adoption of a new technology or a new product. This could be the case if different controllers use the same technology for the same purposes: for instance, if different municipal authorities set up a similar CCTV system in comparable public areas.[52] It could also be the case if different controllers use the same technological product (e.g. a piece of hardware or software) to collect data,

[50] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 18.
[51] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 7.
[52] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 7.

provided that they carry out their own DPIA with regard to the subsequent specific use that they make of such collected data.[53]

In these cases, the different controllers could decide to carry out a joint DPIA. Otherwise, if one of them (e.g. the producer on an IoT device) has already performed a DPIA, then such a DPIA can be used by the other controllers as well. This last scenario requires, however, that the first controller who has carried out the DPIA be willing to share the necessary information to the other interested controllers.

I.3.4 Checklist to carry out a DPIA

Requirements for a DPIA

- Do the processing operations fall into the list of compulsory DPIA issued by the national supervisory authority?

  (The processing operations in question are not only those directly performed by the technology developer, but also those that can be carried out using such technologies.)

- Do the processing operations fall into the list of non-compulsory DPIA issued by the national supervisory authority?

  (The processing operations in question are not only those directly performed by the technology developer, but also those that can be carried out using such technologies.)

- Does the technology allow to perform evaluation or scoring of the data subjects?
- Does the technology allow the collected data to be easily matched or combined with other data sets?
- Does the technology allow the collection of personal data on a large scale?
- Does the technology allow the collection of personal data in contexts that are private (such as devices specifically designed to be used in private houses) or that refer to private situations (such as devices that could register private conversations)?
- Does the technology allow for the collection of sensitive personal data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health, sex life or sexual orientation) or data relating to criminal convictions and offences?
- Does the technology allow for the collection of personal data whose leak could risk damaging the data subject (e.g. financial data that could be used for payment frauds)?

[53] Art. 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, p. 7.

- Does the technology allow the collection of personal data referring to vulnerable subjects (e.g. of patients in hospitals, of employees in the working environment, of children)?
- Does the technology allow to observe, monitor or control data subjects in a systematic way?
- Does such control take place in a publicly accessible area?
- Does the technology allow the data subjects to be aware of the monitoring in process?
- Is the data subject able to avoid such monitoring and control?
- Does the technology allow (full or partial) automated-decisions to be taken with regard to the data subjects?
- Do such decisions affect legal rights of the data subjects (for instance, if the data collected by the device allows to detect alleged non-performance of the data subject and therefore prevents the device to work properly)?
- Do such decisions similarly significantly affect the natural person (for instance, if the collected data can be used to deny the data subject access to essential services, such as health, education or financial services)?
- Does the technology allow for human intervention in the decision process?

  If yes, is such human intervention enough to prevent risks to the rights of the data subjects?
- Is the technology that I am developing new in terms of the potential impact on data subjects?

How to carry out a DPIA

- Am I using a product/component developed by others who have already carried out a DPIA?

  If yes, check whether the producer is willing to share the DPIA and integrate such a DPIA in your own assessment.
- Am I developing a technology similar to others that are being developed?

  If yes, consider the possibility to carry out a joint DPIA.
- Are there codes of conduct that could be taken into account?
- Have I clearly identified the nature, scope, context and purposes of the processing operations?
- Have I identified the assets on which the personal data rely (e.g. hardware, software, people, paper…)?
- Have I consulted all the subjects that are involved in the processing operations (e.g. the DPO, the processors)?
- Is it feasible to consult the data subjects or their representatives on the impact of the technology on their rights and interests? If yes, have I done so?

- Have I envisaged measures to restrict the collection and further processing and storage of data to what is strictly necessary for the purposes of the processing?
- Does the technology makes it possible to provide the data subject with all the necessary information regarding the processing?
- Does the technology allow data subjects to exercise their right to portability?
- Does the technology allow the collected data to be modified and erased?
- Have I clearly identified the risks to the rights and freedoms of natural persons?
- Have I assessed the severity of such risks?
- Have I assessed the likelihood of such risks?
- Have I identified specific measures for each of the assessed risks?
- Have I identified measures to mitigate risks of illegitimate access, modification or disappearance of the data collected by the devices?
- Is it possible to publish the DPIA partially or in a summarised way without hindering the rights of the technology developers or of the data subjects?
- Are the measures that I have designed sufficient to mitigate the risks to the rights and freedoms of the data subjects? If the answer is no, have I consulted the national supervisory authority?

I.4.1 Finding out the PESIA value: The analysis of the case law

The PESIA model is based on the common ethical values recognised by international charters of human rights and fundamental freedoms. This common ground can be defined on the basis of the results of the analysis of the decisions concerning data processing adopted by the European courts (European Court of Justice and Europe Court of Human Rights) and Data Protection Authorities, which are discussed in the following sections.

I.4.1.1 The jurisprudence of the European Courts: The ECHR case law

The European Court of Human Rights (ECtHR) has confronted the issues related to personal data use from the angle of Article 8 of the European Convention of Human Rights (ECHR), which states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." Art. 8 further sets forth procedural safeguards, stating that "[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Article 8 is not the only provision contained in the ECHR which could be used to afford protection to personal data.[54] However, the Court has gradually invoked Article 8 to such end, due to the expansive nature of this provision and to the proximity of the right to privacy to the right to the protection of personal data. Article 8 has also been applied to protect different kinds of interests and rights, ranging from privacy rights to data protection, from personality rights such as personal identity and reputation to family rights, from the right to property to environmental rights.[55]

During this decade-long evolution, the Court has used Article 8 to protect personal information in different contexts. The provisions contained in the ECHR are of a general nature: they do not dictate strict rules but general principles, which must be translated into stricter rules by the Court when applying them to specific cases. In the interpretation of such provisions, ethical principles, which are often incorporated in general legal norms, guide the decisions of the Court.

A first branch of cases regarding data protection concerns surveillance, which is the first instance in which data protection has been tackled under Article 8 ECHR.

The ECtHR case-law usually concerns surveillance for criminal investigation purposes carried out with different means, such as postal interception, telephone

[54] See Paul de Hert, *Human Rights and Data Protection. European CaseLaw 1995–1997 [Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955–1997*] (Jaarboek ICM, 1997 Antwerpen, Maklu, 1998) 91.

[55] See Bart van der Sloot, Privacy as Personality Right: Why the ECtHR's Focus on Ulterior interests Might Prove indispensable in the Age of "Big Data", (2015) 31(80) Utrecht Journal of International and European Law.

tapping, listening and video devices.[56] Issues particularly arise when those means are covert and surveillance is thus secret.

As regards the cases in which surveillance is allowed, their identification is up to the States' margin of appreciation, provided that they respect the following principles. Given that surveillance negatively impacts the rights to privacy and data protection, there has to be a legitimate purpose and the interference must be proportionate. Criminal investigation usually amounts to legitimate purpose and constitutes the case which more often draws the attention of the Court.

Regarding the proportionality requirement, the ECtHR evaluates the kind of rights and interests affected by surveillance in order to strike a balance between these rights and the legitimate purposes underpinning surveillance. To this respect, the more the interests of the individual refer to sensitive situations, the less surveillance is admitted: such situations could refer, for instance, to gatherings with family and friends while in prison,[57] medical correspondence,[58] consultations between a detainee and his lawyer.[59] In some cases, the ECtHR investigates whether further rights risk being impaired by surveillance, such as the right to access to justice in case national authorities intercept correspondence from a detainee to the Court.[60]

In ECtHR case-law, surveillance usually refers to activities carried out by public bodies. There are some instances in which it is private actors who carry out surveillance activities: this is the case of employers surveilling employees using telephone and email interception and video-cameras on the workplace.[61]

The Court states that the need to control what employees do when working does not justify, *per se*, surveillance, but there must be some other legitimate reason, such as the suspicion that the employee is in breach of contract. Moreover, surveillance must be restricted to what is necessary to reach its legitimate purposes, it must be the only effective measure and, in any case, private and social life of employees on the workplace cannot be reduced to zero.

Moreover, when assessing if the intrusion on employees is proportionate, the Court identifies some elements which must be taken into account, such as the degree and

[56] See Klass and others v. Germany, 6 September 1978; Malone v. The United Kingdom, 2 August 1984; Kruslin v. France, 24 April 1990; Halford v. The United Kingdom, 25 June 1997; Lambert v. France, 24 August 1998; Amann v. Switzerland, 16 February 2000; P.G. and J.H. v. the United Kingdom ,25 September 2001; Taylor-Sabori v. the United Kingdom, 22 October 2002; Allan v. the United Kingdom, 5 November 2002; Cotlet v. Romania, 3 June 2003; A. v. the United Kingdom, 17 July 2003; Matwiejczuk v. Poland, 2 December 2003; Matheron v. France, 29 March 2005; Vetter v. France, 31 May 2005; Wisse v. France, 20 December 2005; Copland v. United Kingdom, 3 April 2007; Liberty and others v. United Kingdom, 1 July 2008; HR, Bykov v. Russia, 10 March 2009; Szuluk v. The United Kingdom, 2 June 2009; Iordachi and others v. Moldova, 14 September 2009; HR, Uzun v. Germany, 2 September 2010; Kennedy v. The United Kingdom, 18 May 2010; Association "21 Décembre 1989" and Others v. Romania, 24 May 2011; Shimovolos v. Russia, 21 June 2011; Dragojević v. Croatia, 15 January 2015; Pruteanu v. Romania, 3 February 2015; R.E. v. United Kingdom, 27 October 2015; Roman Zakharov v. Russia, 4 December 2015; Szabó and Vissy v. Hungary, 12 January 2016.

[57] See Wisse v. France, 20 December 2005.

[58] See Szuluk v. The United Kingdom, 2 June 2009.

[59] See R.E. v. United Kingdom, 27 October 2015.

[60] See Cotlet v. Romania, 3 June 2003; Matwiejczuk v. Poland, 2 December 2003; Pisk-Piskowski v. Poland, 14 January 2005

[61] See Köpke v. Germany, judgment of 5 October 2010; BĂRBULESCU v. ROMANIA 5 September 2017; CASE OF ANTOVIĆ AND MIRKOVIĆ v. MONTENEGRO, 28 November 2017; López Ribalda and others v. Spain, 9 January 2018.

kind of the interference (for instance, it is easier to justify the interception of the flow of communications rather than the monitoring of their content), whether employees have been warned in advance and the existence of other safeguards.

A second set of cases concerns the collection and retention of personal information (such as photographs and fingerprints, or information about the individual's activities) by public authorities for criminal investigations or proceedings or for administrative purposes[62].

As this amounts to an interference with the rights protected by the Convention, the collection, retention and use of the information shall be justified by a legitimate purpose. The Court has deemed that such interference is legitimate, for instance, to prevent terrorism and crime, to assess a person's suitability for employment on a post of importance for national security or to assess the eligibility for benefits.

The interference shall also be proportionate and the law should not allow blanket provisions. Among the factors to take into consideration, are the time extension of the data retention (to be evaluated in connection with its purpose), the seriousness of the crime of which the data subject is accused, the circumstance that the data subject is a mere suspect or has been convicted. For instance, a twenty-five-year retention of data regarding the suspect of the theft of a book is not legitimate,[63] while it is legitimate to store data relating to people convicted of sex offences for thirty years.[64]

In any case, the law must provide for clear grounds and there shall be some procedural safeguards. In particular, data subjects must be granted access to their data and information shall be updated in order to reflect the current situation.

Regarding the right to access data stored by public authorities, issues arise when the data relating to an individual also contains information of third parties. In such cases, the ECtHR protects the right to access if the information is necessary to pursue interests connected to the private and family life of the applicant, sometimes requiring that an independent body decide the matter.[65] This is the case, for instance, of requests to access social service records relating to the applicant's childhood or to disclose the identity of the applicant's biological mother.

The above cases regard data processing carried out by public authorities, as it is directly taken into consideration by Article 8 ECHR. However, under the doctrine of

[62] See McVeigh, O'Neill and Evans v. the United Kingdom, 18 March 1981; Leander v. Sweden, 26 March 1987; Kinnunen v. Finland, 15 May 1996; HR, Z. v. Finland , 25 February 1997; Anne-Marie Andersson v. Sweden, 27 August 1997; Amann v. Switzerland, 16 February 2000; Rotaru v. Romania, 4 May 2000; Van der Velden v. the Netherlands, 2006; Turek v. Slovakia, 14 February 2006; Segerstedt-Wiberg and Others v. Sweden, 6 June 2006; Haralambie v. Romania, 27 October 2009; Cemalettin Canlı v. Turkey, 18 November April 2008; S. and Marper v. the United Kingdom, 4 December 2008; B.B. v. France, Gardel v. France, M.B. v. France, 17 December 2009; Dalea v. France, 2 February 2010; Mikolajová v. Slovakia, 18 January 2011; Shimovolos v. Russia, 21 June 2011; Khelili v. Switzerland, 18 October 2011; Nada v. Switzerland, 12 September 2012; M.M. v. the United Kingdom, 13 November 2012; M.K. v. France, 18 April 2013; Brunet v. France, 18 September 2014; Zaichenko v. Ukraine, 26 February 2015; M.N. v. San Marino, 7 July 2015.

[63] See M.K. v. France, 18 April 2013.

[64] See B.B. v. France, Gardel v. France, M.B. v. France, 17 December 2009.

[65] See Gaskin v. The United Kingdom, 7 July 1989; McMichael v. The United Kingdom, 24 February 1995; M.G v. the United Kingdom, 24 September 2002; Odièvre v. France, 13 February 2003; Godelli v. Italy, 25 September 2012.

positive obligations,[66] States are required to grant that the rights protected by the Convention are not infringed not only by public bodies, but also by private actors. Therefore, States have to put up the necessary safeguards in order to prevent the impairment of such rights and provide for sufficiently deterrent measures.

A set of cases in which the ECtHR has affirmed the protection of Article 8 against private parties regards the publication of personal information on the media.[67]

In this case, the protection of private life needs to be balanced against freedom of expression, which is also protected by the ECHR (Article 10). To such end, the Court usually requires that there be a general interest underpinning the publication of personal information. Other elements to take into consideration are the kind of information published (for instance, publication of photographs should be more restricted than other kind of information;[68] home address constitutes sensitive information even if it refers to famous persons,[69] as well as health information),[70] the qualities of the data subject (there are less restrictions if it is a public person, more if a minor is involved),[71] the effects of the publication (for instance, the publication may not be legitimate if it facilitates the access to data even though those data are already public).[72]

The State has therefore to ensure that data subjects are protected against private parties who violate individual rights under Article 8 ECHR. There are different means to reach such goal, such as providing for adequate damages if the press illegitimately publishes personal information[73] or requiring that an internet service provider reveals the identity of those who have illegally published personal information.[74]

Regardless of whether information is collected by public authorities or private parties, the Court gives particular attention to information concerning health conditions and medical records.[75] Processing of health data seems to be legitimate only if it is

[66] See Alistair Mowbray (2004) The Development of Positive Obligations under the Europena Convention on Human Rights by the European Court of Human Rights [Bloomsberg Publishing] 127-188.

[67] See Z. v. Finland, 25 February 1997; Peck v. the United Kingdom, 28 January 2003; Von Hannover v. Germany, 24 June 2004; Sciacca v. Italy, 11 January 2005; Perrin v. The United Kingdom, 18 October 2005; Biriuk v. Lithuania, 25 November 2008; Cemalettin Canlı v. Turkey, 18 November April 2008; K.U. v. Finland, 2 December 2008; Flinkkilä and Others v. Finland, 6 April 2010; Saaristo and Others v. Finland, 12 October 2010; Mosley v. the United Kingdom, 10 May 2011; Avram and Others v. Moldova, 5 July 2011; Axel Springer AG v. Germany, 7 February 2012; Von Hannover v. Germany, 7 February 2012; Kurier Zeitungsverlag und Druckerei GmbH v. Austria (No. 2), 19 June 2012; Mitkus v. Latvia, 2 October 2012; Alkaya v. Turkey, 9 October 2012; Verlagsgruppe News GmbH and Bobi v. Austria, 4 December 2012; Khmel v. Russia, 12 December 2013; Satamedia v. Finland, 21 July 2015; Annen v. Germany, 26 November 2015.

[68] See Verlagsgruppe News GmbH and Bobi v. Austria, 4 December 2012.

[69] See Alkaya v. Turkey, 9 October 2012.

[70] See Z. v. Finland, 25 February 1997; Biriuk v. Lithuania, 25 November 2008; Mitkus v. Latvia, 2 October 2012.

[71] See Kurier Zeitungsverlag und Druckerei GmbH v. Austria (No. 2), 19 June 2012.

[72] See Satamedia v. Finland, 21 July 2015.

[73] See Biriuk v. Lithuania, 25 November 2008; Avram and Others v. Moldova, 05 July 2011.

[74] See K.U. v. Finland, 2 December 2008.

[75] See Z. v. Finland, 25 February 1997; Anne-Marie Andersson v. Sweden, 27 August 1997; M.S. v. Sweden, 27 August 1997; L.L. v. France, 10 October 2006; I. v. Finland, 3 April 2007; I. v. Finland, 17 July 2008; Biriuk v. Lithuania, 25 November 2008; K.H. and others v. Slovakia, 28 April 2009; Szuluk v. The United Kingdom, 2 June 2009; Gillberg v. Sweden, 3 April 2012; Mitkus v. Latvia, 2 October 2012; P. and S. v. Poland, 30 October 2012; Zaichenko v. Ukraine, 26 February 2015.

strictly necessary to reach legitimate purposes: for instance, it may be allowed the transmission of health data from one public body to another if it is necessary for administrative proceedings,[76] as well as the processing for scientific research purposes.[77]

Moreover, adequate safeguards must assist the processing, such as the restriction of unauthorized parties to access medical information (for instance, hospitals shall provide that only authorized personnel have such access),[78] time limits and pseudonymisation techniques.[79] Interception of communication regarding health conditions[80] and press publication should also be restricted. Finally, as regards the access to one's own medical data, it should be granted without any restriction.[81]

Due to the nature the ECHR, which is formulated in terms of broad principles rather than strict rules, the Court has a large margin of interpretation. When assessing whether there has been an interference with the rights protected under Article 8 and whether the interference was legitimate, the Court proceeds to balancing opposing interests. In doing so, it refers, even if not always explicitly, to ethical and social values, which are taken into account in translating Article 8 in rules of conduct. We will therefore enucleate the values which seem to emerge more strongly from the reasoning of the Court.

Self-determination as a moral and social value to be protected consists in the possibility for individuals to freely determine the development and carrying on of their daily activities and decide the kind of person they want to become. If individuals are monitored, they risk not to feel free to carry on their activities as they would normally do, nor to freely develop their personalities and pursue their aspirations.

This could happen, for instance, if the media continuously publish photos of individuals, even if they regard famous persons in public situations: such frequent monitoring has a moral and social impact which is judged negatively by the Court.[82] The same happens when media publish the photograph of an individual instead of just releasing the news:[83] this leads to the person in question to be recognizable, which could cause distress and hinder self-determination. Similarly, the publication of the full name of a minor victim of a crime risks impairing her possibility to overcome the experience and evolve her personality.[84] Another case involving the media, concerns the publication of tax personal information,[85] which could have negative consequences on the individuals involved in terms of distress and lack of self-determination in relation to other people.

Another set of cases judged by the Court regards the monitoring of emails, internet usage and telephone communications of employees by employers. Here there is a

[76] See M.S. v. Sweden, 27 August 1997.
[77] See Gillberg v. Sweden, 3 April 2012.
[78] See I. v. Finland, 3 April 2007; I. v. Finland, No. 20511/03, 17 July 2008.
[79] See Peruzzo and Martens v. Germany, 4 June 2013.
[80] See Szuluk v. The United Kingdom, 2 June 2009.
[81] See K.H. and others v. Slovakia, 28 April 2009.
[82] See ECtHR, Von Hannover v. Germany, 24 June 2004.
[83] See ECtHR, *Verlagsgruppe News GmbH and Bobi v. Austria*, 4 December 2012.
[84] See ECtHR, Kurier Zeitungsverlag und Druckerei GmbH v. Austria (No. 2), 19 June 2012; ECtHR, *P. and S. v. Poland,* 30 October 2012.
[85] See ECtHR, Satamedia v. Finland, 21 July 2015.

particular imbalance due to the working relationship that makes it even more difficult for monitored employees to freely develop their personality on the workplace.[86] The social and private life of employees cannot in any case be reduced to zero, not even on the workplace: this is clearly meant to preserve self-determination of employees in the construction of their private sphere and in the development of their relations.[87] Otherwise, it would be very difficult for individuals, who spend most of their time on the workplace, to cultivate relationships and develop a private life.

The same can be said of video-surveillance of employees, the use if which is strictly limited and controlled by the Court.[88]

Issues involving self-determination also arise in cases of storing personal information in databases, such as records of criminal offences or investigations, for an excessive period of time, or when such information is not updated.[89] In these cases, individuals are impaired in their ability to overcome their past experiences and in the evolution of their personality. This also risks hindering relations with other people, who could have prejudices due to the information stored in the databases.

Self-determination also comes into play in the relations with other people, in the sense that the processing of data should not hinder the freedom to have contacts and develop relationships. For instance, the Court stated that the surveillance of detainees in the parlours dedicated to meetings with visitors (in particular, relatives) violates their right to private life.[90] This is because the collection of data would, in this case, unduly influence the social and family life of detainees, who would not feel free to have normal relationships with visitors if they know they are being monitored. The same can be said of employees, who are not free to maintain and develop social relations if they are constantly being monitored on the workplace.[91]

Freedom and self-determination are also protected in professional relationships, which need to develop freely without constraints deriving from external monitoring. For instance, the confidentiality between a lawyer and his client deserves protection,[92] as otherwise the lawyer would be hindered in exercising his professional activity and individuals would be inhibited in seeking the advice of a lawyer. Relationships between people, also of a professional nature, constitute a value which needs to be preserved.

In some instances, the delicate nature of the relation is taken into account, as in the relationship between a doctor and his patient. The Court has indeed stated that the correspondence between a detainee and his doctor must not be monitored.[93] The social and moral values underpinning such judgement are the dignity of the data subject, as the information in question regards an intimate aspect of his life, but also

[86] See ECtHR, Copland v. United Kingdom, 3 April 2007.
[87] See ECtHR, Bărbulescu v. Romania, 5 September 2017.
[88] See ECtHR, Köpke v. Germany, judgment of 5 October 2010; ECtHR, Antović and Mirković v. Montenegro, 28 November 2017.
[89] See ECtHR, Mikolajová v. Slovakia, judgment of 18 January 2011; ECtHR, Khelili v. Switzerland, judgment of 18 October 2011; ECtHR, M.M. v. the United Kingdom, 13 November 2012; ECtHR, *M.K. v. France*, 18 April 2013; ECtHR, *Brunet v. France*, 18 September 2014.
[90] See ECtHR, Wisse v. France, judgement of 20 December 2005.
[91] See ECtHR, Copland v. United Kingdom, 3 April 2007.
[92] See ECtHR, Niemietz v. Germany, judgment of 16 December 1992; ECtHR, Yuditskaya and Others v. Russia, 12 February 2015; ECtHR, R.E. v. United Kingdom, 27 October 2015.
[93] See ECtHR, Szuluk v. The United Kingdom, judgment of 2 June 2009.

his self-determination, as the monitoring could inhibit the development of a free relationship with the professional.

The values of self-determination and **personal identity** also emerge in cases where the individual wants to access information regarding herself. This is crucial to allow the individual to know about her roots or about her past experiences in order to freely develop her personality. Cases decided by the Court regard, for instance, requests to access data regarding her life as a child in foster care[94] and to know the identity of the biological mother.[95]

Finally, freedom as a social and moral value can also be considered as freedom from unwanted interferences and disturbances which could annoy the individual in her daily life. For instance, freedom in such sense could be impaired if the media publish the address of a famous person.[96]

In the cases concerning government surveillance, self-determination and freedom are strictly linked to the need of **avoiding social control**. The impact of large-scale surveillance carried out by public authorities is considered not only from the point of view of single individuals, but also from the broader perspective of society at large. The social impact to be avoided is the creation of a society in which the government is able to control all aspects of the life of the individuals, whose freedom and autonomy must instead be preserved.

Another value which seems to emerge from the ECtHR case-law is **dignity**, which consists in the respect that needs to be paid to individuals as human beings.

The value of dignity emerges in cases of publication by the media of personal information. When such information regards the intimate sphere of the individual and could cause embarrassment if known by third parties, such as information regarding health conditions,[97] than dignity is impaired. Dignity is also impaired when the continuous publications of photos (for instance, of famous individuals) "induces in the person concerned a very strong sense of intrusion into their private life or even persecution".[98]

Dignity also emerges in those cases in which the Court affirms the protection of an intimate sphere that cannot be impaired by data processing, such as health information. This kind of data need stronger protection,[99] as their dissemination could lead to discriminatory practices or, more simply, to embarrass and distress the individuals concerned.

Dignity is also involved in cases regarding monitoring of employees on the workplace. The Court has indeed referred, as one of the criteria to assess the legitimacy of such practices, to the intrusiveness of the technology used to control employees.[100] Underlying such statement, there seems to be the need to preserve

[94] See ECtHR, Gaskin v. The United Kingdom judgment of 7 July 1989; ECtHR, M.G v. the United Kingdom judgment of 24 September 2002.
[95] See ECtHR, Odièvre v. France, 13 February 2003; ECtHR, Godelli v. Italy, judgment of 25 September 2012.
[96] See ECtHR, Alkaya v. Turkey, judgment of 9 October 2012.
[97] See ECtHR, Z. v. Finland judgment of 25 February 1997; ECtHR, Biriuk v. Lithuania, 25 November 2008; ECtHR, Mitkus v. Latvia, judgment of 2 October 2012.
[98] See ECtHR, Von Hannover v. Germany, 24 June 2004.
[99] See ECtHR, I. v. Finland, 17 July 2008.
[100] See ECtHR, Köpke v. Germany, judgment of 5 October 2010.

an intangible sphere of the individual, who cannot be controlled in ways that could hinder her dignity, as would be the case if intrusive technology were used.

Finally, the Court gives large importance to procedural values, such as **transparency** and **participation**. These values are juridically declined as procedural safeguards in the processing of personal data in order to ensure foreseeability *ex ante* and the possibility *ex post* to control whether the interference was legitimate. However, they also point to an underlying social stance, that individuals be involved in the processing of personal data to maintain **control** over their information.

Such control is aimed at preserving other values, such as self-determination and freedom. In addition, control over personal information could be considered as a value *per se*, since individuals give an increasing importance to being able to control their own data. Lack of control seems indeed to lead to distress and distrust towards data collectors.

I.4.1.2 The jurisprudence of the European Courts: The ECJ case law

The Court of Justice of the European Union (ECJ) has the task of interpreting EU law and ensuring its consistent application among Member States. The Court has therefore intervened on several issues related to European data protection regulation. The number of cases is however smaller that the ECtHR's decisions on the matter, and often involves technical legal issues regarding the interpretation of European norms or infringement procedures against Member States that have not implemented EU legislation,[101] which fall outside the present scope.

As the ECtHR, also the ECJ has been called to interpret general clauses and to balance competing interests. European data protection regulation, mainly provided for by Directive 95/46/EC, contains several general principles which need to be enacted not only by each national legislator, but also through judicial interpretation.

Moreover, European regulation must comply with the Charter of Fundamental Rights of the European Union, which under Article 8 expressly recognises the right to the protection of personal data, stating that "[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Article 52 (1) further states that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." The ECJ therefore also ensures that European legislation and its national applications comply with the Charter.

[101] See Several infringement procedures regard the failure to implement sufficient safeguards to ensure data protection authorities' independence: C-614/10, Commission v. Austria, 16 October 2012; C-288/12, Commission v. Hungary, 8 April 2014.

The juridical approach adopted by the ECJ is similar to that of the ECtHR. First, interferences with the right to data protection need to be justified by a legitimate purpose which should have a clear legal basis; second, interferences shall be proportionate considering the different interests involved in each case. In balancing competing interests, the Court adopts the criteria of necessity and data minimisation, under which data can be processed only if strictly necessary for the legitimate purposes of the controller.[102]

Underpinning such legal reasoning, it is possible to identify moral and social values which guide the decisions of the Court. However, as mentioned, many cases concern technical issues which are resolved through mere legal reasoning and are therefore difficult to analyse for the purposes of this study.

Self-determination and freedom also emerge from the ECJ case-law. A case in which these values are clearly taken into account regards the request of delisting one's own name from online search engines.[103] The value that could be negatively impacted by these practices is the possibility for the individual to develop her personality overcoming past events and her freedom to cultivate relations that are not influenced by what happened in the past.

Self-determination, in the sense that publication of personal information should not constrain individuals in their relationships with other people and in the pursuing of their activities, also emerges when the Court assesses the legitimacy of publishing tax personal information.[104] In leaving such assessment to national authorities, the Court shows that there are some critical issues underlying this matter, as social and moral values are involved. The same can be said of the case regarding the publication of information on public funds received by natural persons.[105]

The Court also considers as a value the **freedom** to carry out one's own activities without being constrained by the fact that personal data are collected. This can be seen when the Court assesses the legitimacy of cameras installed to protect private property, stating that they cannot be directed towards public areas without asking for consent.[106] It is therefore taken into account the necessity to preserve the freedom of action of passers-by.

Dignity seems to be another value taken into account by the Court. For instance, when assessing the legitimacy of fingerprinting, among the criteria is whether such practice could cause physical or mental discomfort to the individuals involved.[107] The collection of data must therefore be undertaken in such a way as to avoid disturbance and discomfort to data subjects, in order to preserve their dignity.

The need to protect dignity also emerges when the Court affirms the reinforced protection of health data.[108] Under this perspective, dignity refers to the preservation

[102] See C-524/06, Huber v. Germany, 16.12.2008; C-342-12, Worten – Equipamento para o Lar SA v. ACT (Authority for Working Conditions, 30.5.2013; C-615/13 P. Client Earth et at. v. EFSA, 16.7.2015; T-320/02, Esch-Leonhardt and others v. European Central Bank, 18.2.2004.
[103] See C131/12, Google Spain SL v. AEDP and Mario Costeja, 13 May 2014.
[104] See C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy and Satamedia, 16 December 2008.
[105] See C-92/09, Volker und Markus Schecke GBR v. Land Hessen and C-93/09, Eifert v. Land Hessen and Bundesanstalt fur Landwirtschaft und Ernahrung, 9 November 2010.
[106] See C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 11 December 2014.
[107] See C-291/12, Michael Schwarz v. Stadt Bochum, 17 October 2013.
[108] See C-101/01, Lindquist, 6 November 2003.

of a private and intimate sphere the violation of which could cause distress and unwanted consequences.

Finally, the Court stresses the importance of procedural values, such as **transparency**[109] and **participation**.[110] These point, again, to the importance of control on personal data, which could be considered as a value *per se*.

I.4.2 The jurisprudence of the Data Protection Authorities

In order to find out the driving ethical and social values underpinning the jurisprudence of data protection authorities (hereinafter DPAs), we analysed the decisions adopted by the DPAs of several EU countries. We examined not only the jurisprudence of these authorities, but also the broader bulk of documents they have adopted over the years (guidelines, annual reports, studies etc.).

We circumscribed our inquiry to the countries that have a long historical experience in the field of data protection and are also more active in this field. We selected the DPAs of the following six countries: Belgium, France, Germany, Italy, Spain, and United Kingdom.[111] Considering the influence that social contexts have on the ethical and social values,[112] we selected authorities belonging to systems that have a similar socio-cultural environment (e.g. Italy and Spain, France and Belgium). We also included United Kingdom due to the potential influence of its different legal system.

Since this selection necessarily entails the exclusion of a significant area (mainly the East part of the EU), our analysis also includes the opinions issued and the documents adopted by the Article 29 Data Protection Working Party in order to fill this gap and recover a complete vision at EU level.

The decision not to circumscribe this research to the documents adopted by national DPAs is also due to the relationship characterising data protection claims and technology. In fact, potential prejudices deriving from the use of innovative technologies may have an impact that goes beyond the individual dimension and may be unknown to data subjects, but can be predicted and estimated by the experts at EU level in the context of the activities carried by the Article 29 Data Protection Working Party.

---

[109] See C-201/14, Smaranda Bara et al. v. Presedintele Casei Nationale de Asigurari de Sanatate (CNAS) et al., 1 October 2015; C-362/14, Schrems v. Data protection Commissioner, 6 October 2015.

[110] Participation has been tackled under the right to access, which should be granted for a sufficient period of time (C-553/07, College Van Burgemeester En Wethouders Van Rotterdam v. Rijkeboer, 7 May 2009) and should not be made conditional to the payment of excessive costs (C-486/12, X, 12 December 2013).

[111] For the purposes of this research we considered only the national authorities and not the regional authorities where present (e.g. Spain and Germany).

[112] See, Nissenbaum H., *Privacy in Context. Technology, Policy and the Integrity of Social Life* (Stanford, 2010); Merry S. E., *McGill Convocation Address: Legal Pluralism in Practice*, (2013), 59, 1, *McGill Law Journal*, available at: *http://lawjournal.mcgill.ca/userfiles/other/75931-Article__1___Merry.pdf*; Bygrave L. A., *Privacy Protection in a Global Context – A Comparative Overview*, (2004), 47, 319, *Scandinavian Studies in Law.*

Regarding the examined documents,[113] there are differences in their amount and nature on national basis. This is due to the variety of powers that can be exercised by national DPAs, the different nature of their acts and policy approaches.

In this regard, the documents from the French, Italian, and Spanish authorities are mainly decisions adopted by these authorities, while in the case of UK DPA only a limited number of decisions is available, since ICO's competences are focused on supporting data controllers. In this case, we therefore examined the guidelines provided by this authority in different sectors.

With respect to the Belgium authority, we considered opinions, recommendations and information provided over the years by the national DPA, but not decisions on specific complaints since, when this research was carried out, this authority lacked decision-making and sanctioning powers. With reference to Germany, the Federal DPA's statements and the minutes of the meetings between the Federal and the Länder DPAs were taken into consideration.[114]

In selecting the keywords to search the documents available on the authorities' websites, we considered the nature of the devices used for data collection (e.g. video surveillance systems, geolocation tools), the nature of spaces where data are collected (e.g. public or private spaces) and the contexts (e.g. work context).

At the end of this initial analysis 730 documents were selected, distributed as follows:

Country	Number of examined documents
Italy	250
France	100
Belgium	80
Spain	70
United Kingdom	100
Germany	30
Art. 29 WP	100

[113] The analysis is based on the document made available on the following DPAs' websites (last accessed April 15, 2018): *https://www.garanteprivacy.it* (Italy); *https://www.cnil.fr* and *https://www.legifrance.gouv.fr* (France); *https://www.privacycommission.be* (Belgium); *https://www.aepd.es* (Spain); *https://ico.org.uk* (United Kingdom); *https://www.bfdi.bund.de* (Germany). The documents adopted by the Article 29 Data Protection Working Party are available here: *https://ec.europa.eu/justice/article-29/documentation/index_en.htm* (documents adopted until November 2016) and *https://ec.europa.eu/newsroom/article29/news-overview.cfm* (documents adopted after November 2016).

[114] These are the so called "National Konferenz". These conferences adopt agreed resolutions which outline the attitude of Federal and Länder privacy authorities with regard to technical, economic and legal issues concerning data processing.

The selected documents were then analysed in detail to identify the most significant cases, in terms of relevance with regard to legal, ethical and social values. Moreover, in this phase, we discarded the redundant documents concerning same issues or adopting a similar argumentative logic. At the end of this examination, the selected decisions to be considered for the purposes of this inquiry were 225 (Belgium 32, France 54, Germany 15, Italy 40, Spain 20, United Kingdom 20, and Article 29 Data Protection Working Party 44).

The analysis of the different documents adopted by DPAs and the considerations expressed by these authorities made it possible to identify a uniform approach driving the jurisprudence of these bodies with regard to the legal, ethical and social values. Despite the fact that some authorities are characterized by different legal and cultural traditions, it was possible to identify a common ground also with regard to ethical and social values.

In light of this, in presenting the results of this inquiry, it is possible to carry out a cross-cutting analysis of the profiles pertaining to the ethical and social values that emerged in the jurisprudence of DPAs. It should be highlighted that whereas the importance of these values is clearly stated in the examined documents, in several cases the relevance of societal issues emerges only indirectly from data protection authorities' observations.

More specifically, these authorities frequently use general data protection principles to safeguard values and interests other than those closely related to privacy and security of personal information. In the adopted decisions, it is therefore possible to find references to principles such as proportionality or necessity which are used to ensure an adequate protection for ethical and social interests.

In particular, in assessing the legitimacy of a given treatment, DPAs take into consideration the different interests that may arise in the specific case. This balancing test of the competing interests becomes the context in which societal issues are considered.

In this regard, although the DPAs' decisions often do not discuss the criteria that underpin this balancing test, it is clear that the DPAs also consider the societal consequences of information processing. More specifically, the DPAs take into account the prejudices that may affect individual self-determination and autonomy, the dignity of natural persons, the right to privacy, and the freedom from discrimination.

- **Self-determination and autonomy**

A significant set of values that emerges in a recurrent way from the examined documents concerns the safeguard of individual autonomy and self-determination. DPAs consider individual autonomy and self-determination in a broad sense, encompassing different aspects, such as the freedom of choices, the freedom of movement, and the freedom of expression. Furthermore, individual autonomy also concerns the free development of human personality and the right to informational self-determination.

Regarding the freedom of choice (encompassing the freedom of movement), limitations may derive from data processing operations that make it possible to

control data subjects' communications and online behaviour (e.g. e-mails, telephone conversations,[115] social networks[116]). According to the DPAs, these forms of monitoring limit data subjects' choices with regard to their behaviour in the online environment or with respect to the opportunity to exchange electronic communications. Other forms of indirect limitations of individual self-determination and autonomy can derive from personal data processing concerning for behavioural advertising purposes.[117]

Forms of surveillance affecting data subjects' freedom of choice can also be put into practice using IoT systems and personal devices, as well as mobile applications[118] (e.g. wearable devices and mobile applications concerning users' health which collect an array of health data that can be used to extract further inferences[119] to be shared with third parties such as insurance companies and employers). In this regard, DPAs have highlighted how personal devices may cause more serious risks to the data subjects' than other electronic devices, because they are used every day and, in most cases, are always switched on (e.g. smartphones, tablets, activity trackers).

Limits to data subjects' individual freedom of choice can also result from the services of the so-called "reputation economy" (e.g. platforms that shows and manage

---

[115] See, among others, Garante per la protezione dei dati personali, February 1, 2018, doc. web n. 8159221; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0464/2013; *Commission de la protection de la vie privée*, avis n. 10/2000, April 3, 2000, *Commission de la protection de la vie privée*, recommandation n. 8/2012, May 2, 2012; Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/DVSystemeArbeitsplatzArtikel/InternetnutzungArbeitsplatz.html*; Ico. Information Commissioner's Office, *The employment practices code Part. 3*; Ico. Information Commissioner's Office, *Quick guide to the employment practices code Ideal for the small business*; Ico. Information Commissioner's Office, *The employment Practices. Code Supplementary Guidance, Part. 3*; Article 29 Data Protection Working Party, WP 55, *Working document on the surveillance of electronic communications in the workplace*, adopted on 29 May 2002.

[116] See, among others, Garante per la protezione dei dati personali, doc. web n. 1567124; Art. 29-Data Protection Working Party, WP 163, *Opinion 5/2009 on online social networking,* adopted on 12 June 2009.

[117] In this sense, see, Article 29 Data Protection Working Party, *WP 171, Opinion 2/2010 on online behavioural advertising,* adopted on 22 June 2010; Article 29 Data Protection Working Party, WP 188, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising,* adopted on 8 December 2011.

[118] See, among others, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, *91st National Konferenz 6th-7th April 2016*, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91DSK_EntschliessungWearables.html?nn=5217228*; Ico. Information Commissioner's Office, *Privacy in mobile apps. Guidance for app developers*, *https://ico.org.uk/media/1596/privacy-in-mobile-apps-dp-guidance.pdf*; Article 29 Data Protection Working Party, WP 223, *Opinion 8/2014 on the on Recent Developments on the Internet of Things,* adopted on 16 September 2014; Article 29 Data Protection Working Party, WP 183, *Opinion 12/2011 on smart metering,* adopted on 4 April 2011; Article 29 Data Protection Working Party, WP 205, *Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force,* adopted on 22 April 2013. Regarding the risks deriving from these instruments, see Mayer-Schönberger V., Cukier K., *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, (2013), 152, London.

[119] See, among others, Montgomery K., Chester J., Kopp K., *Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment*, (2018), 8, 34, *Journal Inf. Pol.*

products and services reviews). DPAs have highlighted how these services can affect the choices of the stakeholders who want to avoid negative opinions.[120]

The autonomy of individuals with respect to their behaviour and freedom of movement is relevant in the cases concerning continuous and invasive monitoring operations (e.g. surveillance systems in private or public spaces[121]).[122] In this regard, we could mention, for example, the cases concerning data processing operations carried out using video surveillance systems in workplaces,[123] schools,[124] and hotels.[125]

An adverse impact on individual freedom of movement may be also due to location services, such as GPS systems used to collect mobility data about private[126] and

[120] See, Garante per la protezione dei dati personali, 24 November 2016, n. 488, doc. web n. 5796783.

[121] Surveillance in public spaces can also be realized using drones (UAV) which may make surveillance operations more difficult to be detected by data subjects. See, Article 29 Data Protection Working Party, WP 231, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, adopted on 16 June 2015; Ico. Information Commissioner's Office, *Drones*.

[122] On the risks of surveillance and social control deriving from the use of new technologies, see, among others, Cate F. H., *Government Data Mining: The Need for a Legal Framework*, (2008), 150, 477, Articles by Maurer Faculty: https://www.repository.law.indiana.edu/facpub/150/; Mantelero A., *Data protection, e-ticketing, and intelligent systems for public transport*, (2015), V, 4, 309, *Int. Data Privacy Law*; Mantelero A., Vaciago G., *The "*Dark Side" *of Big Data*: *Private and Public Interaction in Social Surveillance*. *How data collections by private entities affect governmental social control and how the EU reform on data protection responds*, (2013), 6, 161, *Comp. Law Rev. Int.*

[123] See, for example, Garante per la protezione dei dati personali, 30 ottobre 2013, n. 484, doc. web n. 2908871; Agencia Española de Protección de Datos, Expediente n. 01760/2017; Commission Nationale de l'Informatique et des Libertés, délibération n. 2014-307, 17 July 2014; Ico. Information Commissioner's Office, *The employment practices code Part. 3*; Ico. Information Commissioner's Office, *Quick guide to the employment practices code Ideal for the small business*; Ico. Information Commissioner's Office, *The employment Practices. Code Supplementary Guidance, Part. 3*; Article 29 Data Protection Working Party, WP 89, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, adopted on 11th February 2004*; Article 29 Data Protection Working Party, WP 67*, Working Document on the Processing of Personal Data by means of Video* Surveillance, adopted on 25 November 2002; Article 29-Data Protection Working Party, WP 48, *Opinion 8/2001 on the processing of personal data in the employment context*.

[124] In this regard, it has been particularly highlighted that video surveillance towards minors can lead to serious ethical and social prejudices, as the latter may perceive as normal the subjection to other people's surveillance: see, Article 29 Data Protection Working Party, WP 147, *Working Document on the protection of children's personal data (General guidelines and the special case of school),* adopted on 18 February 2008.

[125] See, Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017.

[126] Garante per la protezione dei dati personali, 7 November 2013, n. 499, doc. web n. 2911484; *Commission de la protection de la vie privée*, Avis n. 27/2009, October 28, 2009; Commission Nationale de l'Informatique et des Libertés, délibération n. 2014-294, 22 July 2014; Commission Nationale de l'Informatique et des Libertés, délibération n. 2010-096, 8 April 2010;. Ico. Information Commissioner's Office, *Data Protection Technical Guidance Radio Frequency Identification*; Konferenz der Datenschutzbeauftragten des Bundes und der Länder, National Konferenz 14th November 2014, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/14112014_EntschliessungPKWMaut.html?nn=5217228; Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 88th National Konferenz 8th-9th October 2014, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_DatenschutzImKfz.html?nn=5217228; Article 29 Data Protection Working Party, WP 115 *Working Party 29 Opinion on the use of location data with a view to providing value-added services,* adopted on 25 November 2005; Article 29 Data Protection Working Party, WP 185, *Opinion 13/2011 on Geolocation services on smart mobile devices,* adopted on 16 May 2011.

company[127] vehicles, smart transportation systems,[128] mobile mapping services,[129] and Wi-Fi tracking services.[130] [131]

In these cases, concerning forms of invasive or extensive monitoring operations, DPAs have highlighted the potential impact of these practices on data subjects' behaviour, since surveillance (or potential surveillance) may induce behaviours in line with data controllers' expectations.[132]

The potential prejudice to individual autonomy can be even more serious when these operations are put into practice in contexts characterized by an imbalance of power between data controller and data subjects. This is the case, for example, of workplaces or data processing operations carried out by public authorities (e.g. crime control and prevention).

As emphasised by DPAs, the constant monitoring of data subjects can also negatively affect freedom of expression in terms of chilling effect. Moreover, surveillance activities do not impact only on the individual sphere, but also on the relational dimension with consequences on the free and full development of individual personality.

This may occur, for example, when video-surveillance systems are used against special categories of individuals (this is the case of video surveillance systems used in schools or in workplaces).[133] Similarly, forms of control over communications or online behaviour may affect data subjects' attitude in expressing their opinions and freely interacting with other people.[134]

Finally, in the examined documents, DPAs often use a broad notion of personal autonomy and self-determination, which encompasses the right to informational self-determination. Examples in this regard concern restrictions on data subjects' use of their own personal data,[135] data subject's consent provided in situations

---

[127] Garante per la protezione dei dati personali, 18 April 2018, n. 232, doc. web n. 9358266; Commission Nationale de l'Informatique et des Libertés, délibération n. 2013-366, 23 November 2013; Article 29 Data Protection Working Party, WP 115 *Working Party 29 Opinion on the use of location data with a view to providing value-added services,* adopted on 25 November 2005.

[128] Article 29 Data Protection Working Party, WP 252, *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)*, adopted on 4 October 2017.

[129] See, Commission de la protection de la vie privée, recommandation n. 05/2010, 15 December 2010.

[130] See, Ico. Information Commissioner's Office, *Wi-fi location analytics*.

[131] See also the practices concerning the collection of information about travellers using airplanes, Article 29 Data Protection Working Party, WP 181*, Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime,* adopted on 5 April 2011.

[132] This is the c.d. chilling effect resulting, in this case, from invasive forms of surveillance, capable of deterring a particular behavior. In this regard, see, Clarke R., *The regulation of civilian drones' impacts on behavioural privacy*, (2014), 30, 3, 287, *Comp. Law & Sec. Rev.*; Penney J. W., *Chilling Effects: Online Surveillance and Wikipedia Use*, (2016), 31, 1, 117, *Berkeley Tech. Law Journ.*; Daniel S. J., *A Taxonomy of Privacy*, (2006), 154, 3, 477, *University of Pennsylvania Law. Rev.*

[133] See above fn. 123 and 124.

[134] Garante per la protezione dei dati personali, 4 June 2015, n. 345, doc. web n. 4211000; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0464/2013; Art. 29 Data Protection Working Party, WP 163*, Opinion 5/2009 on online social networking, adopted on 12 June 2009*.

[135] With reference to the right to information self-determination, see, among others, Bundesverfassungsgericht, 15 December 1983, (1984), 65, 1, *Entscheidungen des Bundesverfassungsgerichts*; Fialova E., *Data Portability and Informational Self-Determination*, (2014),

characterised by imbalance of power[136] or information mandatory required to access services.[137]

- **Dignity**

A foundational value widely protected by DPAs is human dignity. Data subjects' dignity may be negatively affected due to continuous and invasive monitoring operations which can significantly impact on them to the point of cancelling the same image that a person has of herself.

Invasive surveillance practices in the context of the employment relationship (e.g. video-surveillance and geolocation systems, email monitoring and web tracking software)[138] may undermine human dignity, as well as different forms of surveillance

8, 47 *Masaryk U. J.L. & Tech.*; Eberle E. J., *The Right to Information Self-Determination*, (2002), 695, 4, 968, *Utah L. Rev*. Several cases concern profiling and automated decision-making processes, but there are also more peculiar cases such as the one concerning the transfer of a biobank from a controller to another without data subjects' consent; see Garante per la protezione dei dati personali, 6 October 2016, n. 389, doc. web n. 5508051. See also Article 29 Data protection Working Party, WP 251*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* adopted on 3 October 2017.

[136] Commission de la protection de la vie privée FAQ*,* *https://www.privacycommission.be/fr/collecte-de-donnees-du-candidat-aupres-du-precedent-employeur-et-de-ses-clients-lenquete-de*; Ico. Information Commissioner's Office, *Quick guide to the employment practices code Ideal for the small business*; Ico. Information Commissioner's Office, *The employment practices code*.

[137] Garante per la protezione dei dati personali, 27 October 2016 n. 439, doc. web n. 5687770; Commission Nationale de l'Informatique et des Libértes, délibération n. 2009-002, 20 January 2009.

[138] Garante per la protezione dei dati personali: 8 September 2016, n. 350, doc. web n. 5497522; Agencia Española de Protección de Datos, Expediente n. E/02689/2012; Ico. Information Commissioner's Office, *The employment practices code,* Part. 3; Ico. Information Commissioner's Office, *Quick guide to the employment practices code Ideal for the small business*; Ico. Information Commissioner's Office, *The employment Practices. Code Supplementary Guidance,* Part. 3; Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Videoueberwachung.html*; Article 29 Data Protection Working Party*, WP 89, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, adopted on 11th February 2004; Article 29 Data Protection Working Party, WP 67, *Working Document on the Processing of Personal Data by means of Video* Surveillance, adopted on 25 November 2002; Article 29 Data Protection Working Party, WP 48, *Opinion 8/2001 on the processing of personal data in the employment context*.

that occur outside the working context[139] (e.g. use of video-surveillance in schools to constantly monitor students' activity[140]).[141]

Negative consequences for data subject's dignity can also derive from the public disclosure of personal information such as data subject's economic or debt situations, which can undermine individual personal and professional reputation.[142] Similarly, DPAs considered that making publicly available the results of personal evaluation judgements can negatively affect human dignity.[143]

- **Privacy**

The safeguard of data subjects' privacy is taken into consideration in many different contexts. Data subject's right to privacy includes, *inter alia*, the safeguard of personal intimate sphere, personal identity and physical integrity.

Respect for the data subjects' intimate sphere is a crucial element to guarantee the protection of individual physical and mental integrity. The need to protect the intimate sphere of individuals comes into consideration, for example, in case of video-surveillance systems (or other monitoring tools) used in areas characterised by a high privacy expectation, such as restrooms or changing rooms.[144]

---

[139] See, among others, Garante per la protezione dei dati personali, 25 January 2018, doc. web n. 7810766, on the use of electronic devices to identify the position of patients within a healthcare-care facility; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0292/2010; *Commission de la protection de la vie privée*, avis n. 27/2009, 28 October 2009; Ico. Information Commissioner's Office, *Data Protection Technical Guidance Radio Frequency Identification*; Article 29 Data Protection Working Party, WP 252, *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)*, adopted on 4 October 2017; Article 29 Data Protection Working Party, WP105, *Working document on data protection issues related to RFID technology*, adopted on *January 19, 2005*; Article 29 Data Protection Working Party, WP175, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications,* adopted on 13 July 2010; Article 29 Data Protection Working Party, WP 180, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, adopted on 11 February 2011*.

[140] Article 29 Data Protection Working Party, WP 147*, Working Document on the protection of children's personal data (General guidelines and the special case of school),* adopted on 18 February 2008.

[141] See also the case of systems that make it possible a permanent localization of private vehicles; see, among others, Garante per la protezione dei dati personali, 7 November 2013, n. 499, doc. web n. 2911484.

[142] Garante per la protezione dei dati personali, 8 June 1999, doc. web n. 40369; Garante per la protezione dei dati personali, 28 May 2015, n. 319, doc. web n. 4131145.

[143] See Ico. Information Commissioner's Office, *Publication of exam results by schools*.; Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/PersonalArbeitnehmerdatenArtikel/NotenspiegelImInternet.html*.

[144] Garante per la protezione dei dati personali, 8 March 2007, doc. web n. 1391803; Garante per la protezione dei dati personali, 24 February 2010, doc. web n. 1705070; Ico. Information Commissioner's Office, *Wi-fi location analytics*; Article 29 Data Protection Working Party, WP 89, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance,* adopted on 11th February 2004; Article 29 Data Protection Working Party, WP 67, *Working Document on the Processing of Personal Data by means of Video* Surveillance, adopted on 25 November 2002; Article 29 Data Protection Working Party, WP 48, *Opinion 8/2001 on the processing of personal data in the employment context*, adopted on 8 June 2017. In this context, see also Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017.

The safeguard of individual intimate sphere is also related to the use of biometric devices, due the nature of collected data,[145] and IoT wearable devices or other devices directly connected to the data subject's body (e.g. smart cars or smart home devices), due to the nature of this relationship.[146]

In the broad context of the safeguard of individual privacy, data subject's identity is also considered as a core value. Identity traditionally concerns different dimensions (i.e. social, physical, and psychological identity) and the safeguard of personal identity covers different profiles such as name, family and ethnic origins, sexual, political and religious orientation.

The notion of personal identity can therefore assume two different meanings. Identity can refer to the set of personal information that makes it possible personal identification, on the one hand, or can refer to the set of information concerning the projection of the individual within the social community, on the other. The latter is related to the interest of a person to be represented in the social life with her real social identity and not to be misrepresented.

In the context of the examined decisions, the safeguard of personal identity mainly regards the first meaning, as demonstrated by the cases concerning the collection of biometric data,[147] which are increasingly used to control access or presence in certain areas, such as in the workplace (to monitor employees' activities) or at school (to prevent access to strangers). Other cases of data processing for identification purposes concern genetic data,[148] online profiling,[149] and the use of personal devices.[150]

Regarding physical integrity as a concrete dimension of privacy, the jurisprudence of the DPAs mainly concerns invasive treatments, such as data processing operations based on implanted RFID devices (e.g. subcutaneous microchips) used to collect and process personal information such as identification data, credit card number or health information.[151]

---

[145] Agencia Española De Protección De Datos, Gabinete Jurídico, Informe 368/2006.

[146] Article 29 Data Protection Working Party, WP 223, *Opinion 8/2014 on the on Recent Developments on the Internet of Things,* adopted on 16 September 2014; Article 29 Data Protection Working Party, WP 183, *Opinion 12/2011 on smart metering*, adopted on 4 April 2011; Article 29 Data Protection Working Party, WP 205*, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force,* adopted on 22 April 2013.

[147] Garante per la protezione dei dati personali, 18 June 2015, n. 360, doc. web n. 4170232; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0392/2011; Commission de la protection de la vie privée, avis n. 17/2008, 9 April 2008; Commission Nationale de l'Informatique et des Libertés, délibération **n 2016-220, 21 July 2016;** Ico. Information Commissioner's Office*, The use of biometrics in schools*; Article 29 Data Protection Working Party, WP193, *Opinion 3/2012 on developments in biometric technologies,* adopted on 27 April 2012; Article 29 Data Protection Working Party, WP 80, *Working document on biometrics,* adopted on 1 August 2003.

[148] Article 29 Data Protection Working Party, WP 91, *Working Document on Genetic Data*, adopted on 17 March 2004.

[149] Art. 29 Data Protection Working Party, WP 163, *Opinion 5/2009 on online social networking,* adopted on 12 June 2009.

[150] Article 29 Data Protection Working Party, WP 192, *Opinion 02/2012 on facial recognition in online and mobile services*, adopted on 22 March 2012.

[151] Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0292/2010; Garante per la protezione dei dati personali, 9 March 2005, doc. web n. 1109493.

- **Non-discrimination**

Discriminatory practices may occur in the context of a variety of data processing operations,[152] such us surveillance activities (e.g. surveillance practices directed, without a justified reason, to control certain groups or categories of subjects due to their gender, ethnic or racial origin).[153] Nevethless, the most relevant forms of discrimination concern decision-making processes and profiling activities,[154] where the collective dimension of data use also becomes important.[155]

In fact, in many cases, the main target of data analysis is not the individual and her profile based on her behaviour, but groups of people or communities. AI and Big Data applications are often used to analyse the nature and to predict the behaviour of these groups for decision-making purposes. In this context, involuntary biases or intentional discrimination may significantly and negatively affect these groups.[156]

---

[152] See also Art. 29 Data Protection Working Party, WP 163, *Opinion 5/2009 on online social networking,* adopted on 12 June 2009.

[153] This kind of prejudices can also occur in the case of data processing operations for online behavioural advertising purposes or based on the information collected via IoT devices. See Article 29 Data Protection Working Party, WP 223, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, adopted on 16 September 2014; Article 29 Data Protection Working Party, WP 171*, Opinion 2/2010 on online behavioural advertising,* adopted on 22 June 2010; Article 29 Data Protection Working Party, WP 188*, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, adopted on 8 December 2011.

[154] See also Article 29 Data protection Working Party, *WP 251, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* adopted on 3 October 2017; Ico. Information Commissioner's Office, *Big data, artificial intelligence, machine learning and data protection*; Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 89th National Konferenz 18th-19th March 2015, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-BigData.html?nn=5217228.

[155] See, Mantelero A., *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, 2016, 32, 241, *Comp. Law and Sec. Rev.*

[156] In this regard, the systems for the analysis of Big Data used to predict the occurrence of crimes in certain areas can be mentioned (see, among others, Perry W. L. et al., *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, (2013), Santa Monica, CA, available at: *https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf*; Robinson D., Yu H., Rieke A., *Civil Rights, Big Data, and Our Algorithmic Future. A September 2014 report on social justice and technology*, (2014), 18–19, available at: *https://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf*), or to subdivide customers according to specific categories by insurance companies or credit institutions (see, Federal Trade Commission, *Credit-Based Insurance Scores: Impacts on consumers of automobile insurance*, Report to Congress – (July 2007), 50, https://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta_report_credit-based_insurance_scores.pdf). In general, with regard to the risk of discrimination that may derive from the analysis of Big Data and automated decision-making procedures, see Council of Europe. 2017. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a; Barocas S., Selbst A. D., *Big Data's Disparate Impact*, (2016), 104, *California Law Rev.*; Custers B., Calders T., Schermer B., Zarsky T. (eds.), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, (2013) Springer; The White House, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, (2014), 51, *https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf*; The White House, Executive Office of the President, *Big Data: A Report on Algorithmic Systems,*

The examined decisions also consider the potential discriminatory effects concerning the use of sensitive data to prevent or restrict data subject's access to certain services or advantages.[157] This is the case, for example, of the collection of genetic data by insurance companies to define the amount of insurance costs on the basis of the insured's potential future health conditions.[158]

I.5 The ethnographic analysis

The ethnographic analysis has been carried out by LSE. The following considerations are based on the internal report provided by Dr Selena Nemorin ("Notes on Values from LSE Ethnography Team") at the end of July 2018.

- **Privacy**

Privacy is, in general, used by IoT developers to describe users' relationship to the data produced by IoT hardware and software. This includes specific discussions on allowing users to access their own collected data (which is also a GDPR condition) or giving clear explanations to users about how the data collected about them is used. The right to be forgotten, as the users' right to delete all their data, is also often mentioned by IoT developers.

In the Deliverable 2.2 it was noted that as far as children are concerned, the concept of privacy usually does not seem to take seriously freedom from advertising. Similarly, bodily integrity when it comes to IoT wearables was also not mentioned as one of the developers' concerns.

With respect to bodily integrity, increased monitoring facilitated through IoT devices is often put forth for overcoming care burden, and easing the life of those in need of these devices. In fact, when it comes to data privacy, it is made less of a concern for vulnerable groups such as the disabled, elderly and persons with dementia, as their care, supposedly, require increased monitoring.

With respect to children, however, it has been possible to identify companies started up by parents who have been concerned with the privacy settings of the available

---

Opportunity, and Civil Rights, (2016), *https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.*

[157] In this regard, we can also recall a decision by the Italian authority concerning the collection of sensitive data made by a real estate agency (such as information suitable to reveal the ethnic or racial origin, religious and sexual orientation, the conditions of health), for the sole purpose of meeting the discriminatory needs of the real estate owners: Garante per la protezione dei dati personali, 11 January 2007, doc. web n. 1381620; see also, *Commission de la protection de la vie privée, recommandation* n. 01/2009, 18 March 2009.

[158] See, Article 29 Data Protection Working Party, WP 91, *Working Document on Genetic Data*, adopted on 17 March 2004. See also the case of sensitive information requested by the employer during the recruitment procedures; see Ico. Information Commissioner's Office, *The employment practices code*, Part. 1, 4; Ico. Information Commissioner's Office, *Quick guide to the employment practices code Ideal for the small business*; Ico. Information Commissioner's Office, *The employment Practices. Code Supplementary Guidance*, Part. 1, 4.

IoT devices in the market for education and care. One such start-up, for instance, was initiated by a father who found out that the baby cameras they were using at home were hacked. He was also increasingly concerned with how the children were monitored and their data kept through these devices. So, he started an edu-tech hardware company for kids.

- **Data protection**

Since GDPR came into force, all the discussions on data protection among IoT developers seem to be dominated by it. GDPR is considered to be the ultimate benchmark for data protection, and as long as companies comply with it (which they have to, to be able to operate in the EU). It is as if, they would not need to consider any other aspects of data protection.

In this regard, vocabulary is missing to identify concerns related to group bias, profiling and discrimination beyond personal data protection.

Similarly, as an implication of GDPR, many companies seem to have moved away from collecting and processing personal data and using “anonymised data” is seen to be a way to ensure data protection. This limits any discussions on data protection.

- **Data ownership**

Data ownership remains an important concern, although there are different arguments about who owns the data: the operating company, software company, the user or whoever pays for it (third parties). In fact, there are now start-up companies which enable users to be able to own their data and trade it with companies as they wish. When asked, whether consumers are able to understand the [real] value of their own data, their answer stands that, there is only one way of finding out, and this is through letting them trade their own data and at least seeing its value.

- **Safety**

There are mainly two meanings associated with safety. The first is usually joined together with security (“safety and security concerns”) and is related to data processing (e.g. sensitive data processing in financial and health sectors). The second is related to protection against harm by IoT devices. Reminding us of discussions on liability and responsibility, questions such as how can IoT devices not cause harm to their users seems to be a key growing concern in the IoT developer community. This concern is especially raised with respect to personal robots (used for care or connectivity at home) in the presence of children, elderly or disabled. One such robotics company for instance mentioned that although their robots are “very secure” and a 80kg person can lean on them with no problem, they are still faced with the problem of what happens if the robot cannot identify and fall from the stairs on a person downstairs (or a children).

- **Security**

Security is understood by IoT developers both in terms of hardware (device) security and software security. During interviews, many people mentioned that IoT products have a bad reputation due to high risks of hacking and security gaps in their designs. This is why implementing security-by-design is often put forth as a solution. However, quickly many companies add that this is very costly for many start-ups and hence often they are not able to work on a security-by-design basis.

Increased monitoring to foster the security of the product (and the consumers) is also mentioned as a value. The more data points an IoT ecosystem have, the more the IoT company can be made aware of potential vulnerabilities and take precautions.

- **Responsibility**

Responsibility is usually related to monitoring the environmental impact of companies, and less about algorithmic accountability or liability.

There is also significant amount of “responsibility forwarding” by which I mean that, software producers do not take responsibility for how the implications of their product when they operate with a certain hardware or similarly, hardware companies argue that it is the responsibility of the software company if the product stops working or is faulty.

Another important observation is related to the implications of changing the core functions of IoT products. For example, an IoT device can be designed to track animals (e.g. sea turtles), in which case it would not need to be GDPR compliant. But what happens when a company buys that device and adapts it to track humans? Where would the responsibility lie in this case? There are ongoing discussions on this matter that we would like to acknowledge.

- **Openness**

In the best-case scenario, many companies mention that open hardware and software with open source code (though not open data for privacy reasons) would be the ideal. However, many companies quickly add that, many start-ups operate in a really competitive market and keeping source code open, or using hardware and software opens them up to various vulnerabilities. A start-up, who produces edu-tech products for museums for instance mentioned that, if they used open hardware, it would be great for consumers to buy and build their own products, but then big corporations would do the same, and they would lose their business in its entirety.

- **Interoperability and Standards**

Interoperability is considered as one of the key values of IoT as mentioned through the ideal of “trusted IoT ecosystem”. However, it is important to stress that it means different things to different persons and organisations.

In general, the idea imagines a future where all IoT devices can talk to one another and third parties would be allowed to connect their clients to the backend of other devices. It also seeks that third-party clients would operate on the same functional

scope on the backend as their own clients. Nevertheless, IoT scene is very competitive and the life cycle of products (and companies) can be very short. Moreover, interoperability also can create significant security and privacy risks for otherwise secure networks and devices, so in reality, interoperability is mentioned as connectedness between a company's own products or products at various life stages.

Many IoT companies mention the invisibility of their IoT devices ("melting to the background") as an important value for seamless integration to the lives of their consumers. Similarly, in industrial IoT field, the invisibility of IoT devices and ubiquitousness of the IoT networks, sensors and devices is mentioned as a desirable feature for the future of technology. Here, the interoperability of the networks and devices through an infrastructure that connects them is mentioned as a significant requirement for this level of integration to happen.

- **Transparency**

With respect to how the use of IoT devices would change, or what would happen to them after a software update, there is significant demand from IoT companies to be transparent about their terms of service. Transparency is understood not necessarily in relation to the inner operations of a company (e.g. business relations, funding bodies which back up the start up in the beginning) but more in terms of device usage and firmware and software upgrades.

- **Social-environmental justice and lifecycle**

Social and environmental justice is often discussed by IoT developers together with the life cycle of IoT products. Not all, but some companies are also concerned with social and environmental justice. These companies especially try to operate on a circular economy basis and emphasise how they would deal with end of life of their own IoT products and how they would be servicing them throughout their lifecycle.

Increasingly there is concern about e-waste created from IoT devices, as the application of the idea is vast, and this means that, a significant amount of IoT products are for testing brilliant ideas which do not necessarily work or get taken up by consumers. Similarly, as it is a growing field, prototypes are usually released as final products every couple of years (e.g. Amazon Alexa, Google Home and similar home assistance IoT products), with the older versions being no longer supported by the companies after one or two new releases. There is significant criticism for less-than transparent practices about how long products would be serviced and what would happen to them at the end of their lives.

Lifecycle also is discussed with respect to how long the companies (are willing to) offer support, provide repairs for components or when software stops working. Also, there are discussions around if the devices can still be employed once the company has finished its operations or gets acquired by another parent company which may or may not support earlier versions.

- **Wellness and care**

Wellness and care are mentioned both as values and product ideals in the IoT scene. This duality is particularly important to pay attention to, as it runs the risk of ethics-washing some of the previously identified concerns with IoT devices. As mentioned above with respect to vulnerable persons, increased monitoring in return for care and wellness tracking is frequently mentioned as a trade-off, which users/consumers are presumed to be happy with.

In general, if an IoT product increases the wellbeing of an individual, it is assumed to be fostering "good". This is why a significant proportion of tech for good companies operate on wellness and care products. There is, however, also wellness washing happening as an economic value. A connected fridge camera start-up for instance, argued that their product would be useful for parents to keep track of what their children are eating in order to overcome obesity or other eating disorders.

- **Ethics as an economic value for the company**

"Ethics washing" is an important term also used by the developers that we have met in the IoT field. There is significant amounts of ethics washing happening, as consumers become more aware of the social, moral and environmental implications of vastly changing technology. So, being identified as an "ethical company" is seen as a branding, a good marketing move for the companies – in a scene which is increasingly competitive. In other words, ethics is assumed to be able to provide an "edge" to the start-ups competing in the IoT field, if their products can be certified as such (be it literally or figuratively).

Part II Towards PESIA

II.1. Introduction

From a **methodological perspective,** the **first challenge** in the development of a general Privacy, Ethical and Social Impact Assessment model concerns the definition of the list of legal and societal (i.e. ethical and social) values that should underpin this model. In this regard, this deliverable combines the outcomes of the legal inquiry with the results of the ethnological analysis, described in the previous sections.

In this light, the development of the guidelines for this model has contributed to better define the boundaries of the legal, ethical and social values and to understand the existing relationship between these different realms. This is also an important starting point for future cross-disciplinary publications by the project members in the field of law and ethics.

In a scenario characterised by different sources of values, coming from the legal and ethnological analysis, it is necessary to outline a common value framework which provides a suitable baseline for the PESIA. This goal was achieved mapping the values and their connections.[159] In this way, this part of our research produced two results: it empirically demonstrated the overlapping between the two different clusters of values (legal and societal) and identified a homogenous list of core values that represent the architecture of the assessment model. The combination of these two results has simplified the values architecture to be used for the PESIA, avoiding redundancy and overlapping between the driving values.

Defining these values is the first step in designing the PESIA model, since values underpinning IoT technologies development should then be transposed in an efficient model which can be easily adopted by developers. For this reason, the PESIA model is built on the previous experience of the PIA/DPIA models, which provide useful reference points and are schemes that data controllers already known. This continuity with the impact assessment schemes used in the field of data protection can facilitate the adoption of the PESIA model by developers.

In this regard, the **second methodological challenge** addressed in our research concerned the harmonization of the different existing PIA/DPIA models.[160] Moreover, since the PESIA also encompasses the assessment of the IoT development with regard to societal values, a **third challenge** is represented by the formulation of a list of questions regarding the ethical and social values.[161] In this field, unlike in the field of privacy impact assessment, there is a lack of pre-exiting models, since the ethical and social impact analysis is taking its first steps in the context of data processing.[162]

[159] See below Section II.2.
[160] See below Section I.2.
[161] See below Section II.3.2.2.
[162] See Mantelero A. 2016. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. 32(2) Comp. Law and Sec. Rev. 238-255;

This deliverable addresses all these three methodological challenges and, in doing so, it provides some **initial guidelines on the development of the PESIA** with a set of questions which represents the result of the mentioned harmonization process.

These questions extensively cover the privacy-focused section of the PESIA and the deliverable provides some indications and an initial set of materials (cases and questions) for the development of the sections concerning ethical and social impacts. According to the development of the research activities described in Tasks 4.3, 4.4 and 5.2, these two sections of the PESIA will be further elaborated in the following months, on the basis of the interaction with the communities of IoT developers to better embed their viewpoints and values in the model.

II.2. Methodology: A map of values

The following two tables summarise the values observed in case law on data processing and in the inquiry carried out in the ethnographic domain,[163] described above in this deliverable. Regarding the legal domain, the values figured out in the empirical analysis of the decisions adopted by courts and Data Protection Authorities should be necessarily integrated by the values enshrined in the GDPR. The latter have not been yet extensively analysed in the case law, due to the recent application of the new regulation. These normative vales mainly concern the following four areas: data protection rights (Artilects 15-22 GDPR[164]), transparency (Artilects 13, 14, 15 and 22 and Recital 71 GDPR[165], see also Article 29 Data Protection Working Party. 2018. Guidelines on transparency under Regulation 2016/679), participation (Artilects 35.9, see also Article 29 Data Protection Working Party. 2017. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[166]) and accountability (Artilects 5.2, 24, 32, 35 and 36 GDPR, see also Article 29 Data Protection Working Party. 2017. Guidelines on Data Protection Officers ('DPOs')[167]).

Vedder, A.H. 1997. Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations. In Moore, G. (ed). Business Ethics: Principles and Practice (Business Education Publishers).

[163] See above Section I.5 (The ethnographic analysis) and Fritsch, E., Shklovski, I., and Douglas-Jones, R. 2018. Calling for a revolution: An analysis of IoT manifestos. In Proceedings of the 2018 ACM Conference on Human Factors in Computing (Montreal, Canada).

[164] More specifically, Article 15 concerns the right of access by the data subject, Article 16 is about the right to rectification, Article 17 regards the right to erasure ('right to be forgotten'), Article 18 recognises the right to restriction of processing and Article 20 recognises the right to data portability (see also Article 29 Data Protection Working Party. 2017. Guidelines on the right to data portability). Articles 21 and 22 regard the right to object and the right not to be subject to a decision based solely on automated processing.

[165] Articles 13 and 14 concern information to be provided to data subject, and Article 15 concerns the right of access by the data subject. Article 22 and Recital 71 are about information to be provided to data subject in case of data processing used in the context of automated individual decision-making.

[166] Pursuant to Article 35.9 "Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations".

[167] Pursuant to Article 5.2 the controller "shall be responsible for, and be able to demonstrate compliance with, paragraph 1" where paragraph 1 mentions the six key principles relating to

Legal Domain – Values	Main goals/issues in the IoT context
Privacy	Safeguarding intimacy, identity, and physical integrity.
Dignity	Avoiding any forms of surveillance or invasive control over individuals using IoT devices. IoT devices shall not be used to collect unauthorised private information or to publicly disclose private facts.
Non-discrimination	Preventing any forms of discrimination.
Autonomy	Safeguarding individual self-determination and freedom of expression.
Data protection rights	Ensuring the rights to access, rectification, erasure and to object with regard to personal data processed by means of IoT devices, and facilitating data portability.
Transparency	Providing access to information concerning data processing.
Participation	Effectively engaging data subjects in data processing design.
Accountability	Effectively addressing security and safety issues, adopting adequate risk prevention strategies and measures.

processing of personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality. From this perspective, also rest of the mentioned articles are relevant, since they concern the responsibility of the controller (Article 24), data security (Article 32) and risk management (Articles 35 and 36).

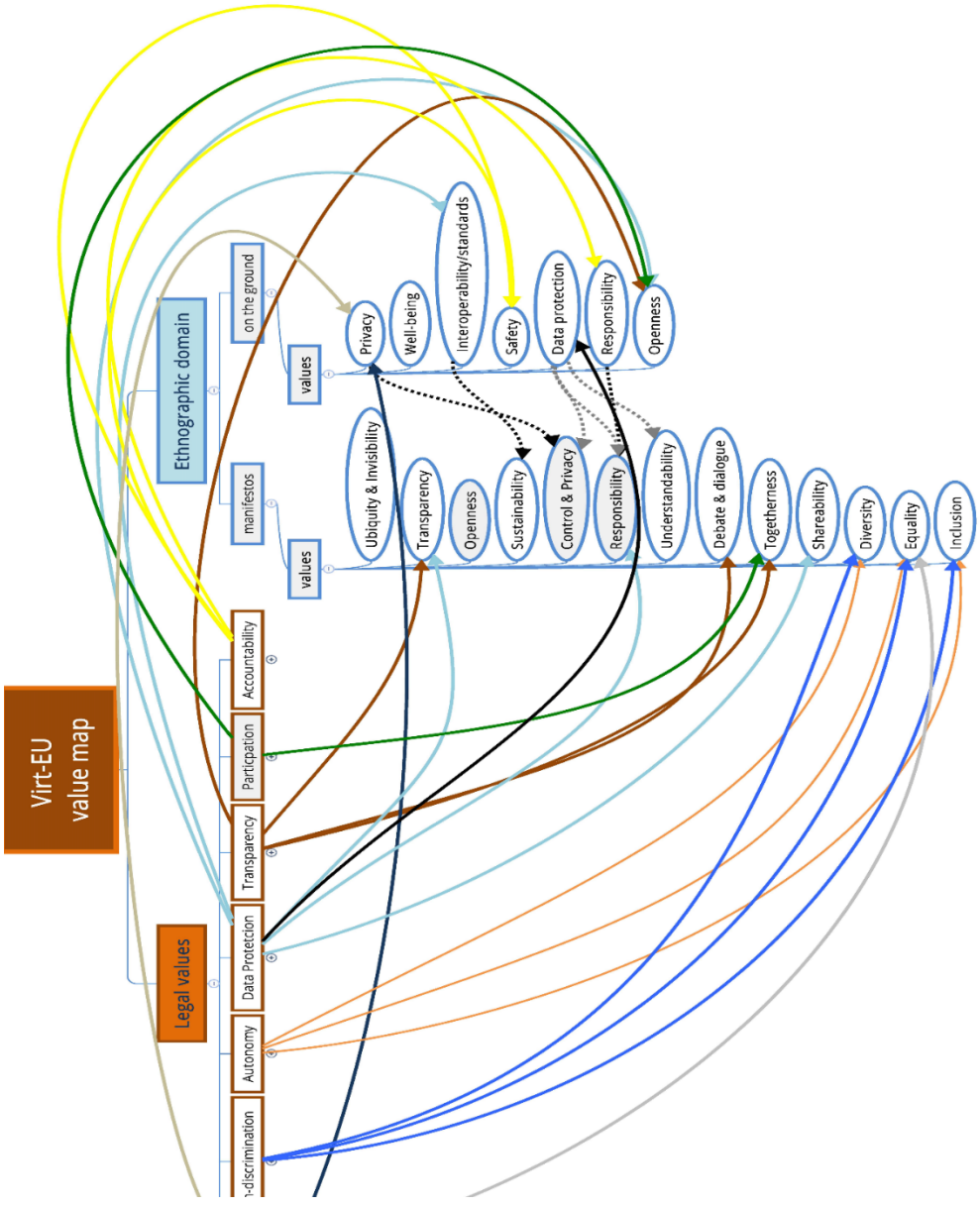
Ethnographic domain - Values	Main goals/issues in the IoT context
Privacy and data protection	Providing users access to their collected data, giving them explanations about how personal information is used, and ensure their right to be forgotten. Issues concerning the distinction between anonymous and personal data.
Well-being	Increase individuals' wellbeing and fostering "IoT for good".
Interoperability	Promoting interoperability as one of the key values to create a trusted IoT ecosystem.
Safety & security	Protecting users against any harm due to IoT devices (hardware and software security).
Responsibility	Strengthening algorithmic accountability/liability.
Openness and shareability	Promoting open hardware and software with open source code.
Transparency and updatability	Encouraging transparency about data operations, device usage and firmware and software upgrades.
Sustainability	Issues concerning the potential impact on social and environmental justice.
Participation	Promoting debate and dialogue (e.g. manifestos).
Inclusion and equality	Considering diversity and inclusion both in IoT development and with regard to users' experience.

The initial analysis of these sets of values focused on their connections and on the overlapping between the different values. The following map visually describes these relationships. In many cases, the different examined contexts (the regulatory framework and the context of the communities of developers) formalise their driving values in different manners.

In this sense, data protection authorities and courts use definitions that are more technical, compared to IoT developers. However, the core values that can be identified in these two realms of our analysis are largely the same. Legal values are echoed in the values pointed out by the developers and vice versa.

In this sense, not only the notion of privacy and data protection are common to the legal context and the context of IoT developers, but they also represent crucial issues in both these fields. Similarly, values such as dignity, non-discrimination, respect of diversity, equality and inclusion are core components of the legal opinions issued by Data Protection Authorities and are considered important values by IoT developers. Moreover, from a technical standpoint, values like openness, shareability and interoperability are constitutive elements of data protection regulations and represent the goals of many IoT projects.

Finally, both from the legal and the IoT development perspectives, there is an emphasis on data gatherers' accountability, which also entails duties in terms of transparency.



This map shows how the two different inquires carried out in the legal and ethnographic domains lead to similar conclusions, converging towards a common set of values. This confirms the possibility to build a values-based model, which is not the result of a mere theoretical and unilateral analysis of our society, but results from an empirical analysis of the legal and social contexts.

The overall conclusion of this study is therefore that these values are existing and effective in the EU society and they can be the backbone for a values-based assessment model which is not only focused on data protection, but also encompasses ethical and social values.

II.3.1 Guidelines for developing PESIA: The main components of the model

The PESIA methodology is a universal methodology, which can be applied in different contexts. It is based on the three different preliminary analyses which have been outlined in the previous sections and have been used to draft the three main blocks of the PESIA (i.e. privacy assessment, ethical assessment and social assessment).

In this regard, it is important pointing out that these three components cannot be addressed in a separate manner and considered as autonomous silos. In this sense, the previous sections describe the interplay between the legal and the ethnographic analysis in defining the different values underpinning this assessment model. Moreover, the ethnological investigation shed light on the manner in which legal constraints are perceived and addressed in real world.

For these reasons, on the basis of the outcomes of this project, the PESIA should be drafted adopting a methodology which combines a thematic approach (focused on the investigated domains) and a crosscutting approach (focused on the values taken into considerations). The following table outlines this approach.

		Value domains		
		P (privacy)	**E (ethical)**	**S (social)**
Investigated domains	**Legal**	PIA/DPIA models	General values outlined in case law (DPAs, ECJ, ECHR) and DPAs' documents **(privacy-related values)**	General values outlined in case law (DPAs, ECJ, ECHR) and DPAs' documents **(privacy-related values)**
	Socio-ethnographic	Developer's perception of legal values and constraints	Specific values pointed out by developers **(a broad array of values)**	Specific values pointed out by developers **(a broad array of values)**

With regard to ethical and social values, as a consequence of the different methodological approaches adopted, the legal analysis described above is mainly focused on privacy-related values, while the socio-ethnographic analysis covers a broader array of values. On the contrary, regarding privacy-focused issues, the legal analysis provides a high level of granularity which can be improved only in a limited manner by socio-ethnographic evidences, which often represent a sort of empirical check of the level of acceptance and applications of legal values.

Following the approach adopted in this project, the outline of a PESIA model can be carried out in different geographical contexts, considering the two mentioned domains and their interaction and contribution to the assessment model, as described above and represented in the following table.

Domain	Target of the analysis	Expected results	Contribution to PESIA
Legal analysis	Legal framework	Mandatory provisions Legal values	Outlining a general model for PIA which is not affected by local implementations of data protection principles
	Case law, DPAs' jurisprudence	Legal values Interplay with ethical and social values	Outlining the core values that should be considered in developing IoT devices both from a legal and a socio-ethical perspective
Socio-ethnographic analysis	Legal compliance	Awareness of legal constraints	Outlining the critical areas to be specifically addressed in the PESIA questionnaire
	Deign approach	Values embedded in IoT design	Completing the values map outlined on the basis of the legal analysis, adding further non-privacy-related values

II.3.2 The architecture

The PESIA is a questions-based model, like the PIA/DPIA model. In fact, a questionnaire can better orient developers, making it possible to segment a complicated assessment in different thematic sections and sub-sections focused on each of the different value domains here considered.

Since IoT developers may not have a specific background in the legal and socio-ethical fields, this values-based approach makes the assessment easier: developers are progressively led through the different issue related to the considered values. In this sense, for example, initial questions about the technological solutions adopted and their purposes facilitate respondents in understanding the following more specific questions on risk management, which are therefore put in an appropriate context.

For this reason, the PESIA model is divided into three thematic sections, focused on privacy/data protection, ethical and social issues, respectively.

The first of these sections is the least innovative one, since represents a synthesis of the existing PIA/DPIA models. However, this section plays an important role in providing a common scheme in a regulatory context were several different models are available at national level, making it difficult for developers to understand their differences and deciding which one should be adopted. In this light, this section on data protection can contribute to the harmonisation of the GDPR-based assessment practices, which represents a key issue in today's regulatory debate in Europe.

The other two sections are the most innovative, since data controllers are not used to have them in the PIA/DPIA models and due to the fact that they focus on values that are not already defined by the law. To better support developers in addressing the novelty of the proposed approach, the PESIA model – in these sections – does not only provide a set of questions, but also some introductive cases which give examples about the societal challenges that are addressed by the different groups of questions.

Compared to the PIA/DPIA models, the PESIA model does not have a threshold, in terms of risk severity and probability. This is due to two different reasons. First, this is a self-assessment model and not a mandatory one. Developers can therefore adopt it also when the potential risk is not high. Second, it is difficult defining a threshold with regard to ethical and social issues, since there are not consolidated measurement criteria in these fields.

Finally, the PESIA aims to cover the entire life circle of the assessed IoT devices and services. In this sense, the PESIA is not different from the other assessment models adopted in the field of data protection. Nevertheless, social and ethical values are affected by a different degree of obsolescence compared to the data protection issues concerning data security, where innovation is frequent and has a significant impact on the adopted solutions.

II.3.2.1 The Privacy section of the model

The first section of the PESIA model is based on the analysis of the existing PIA and DPIA models. This analysis has made it possible to define a general scheme that takes into account the key questions of the main models developed by national and regional Data protection Authorities before (PIA) and after (DPIA) the entry into force of the GPDR.

The following questionnaire represents the result of this first stage of research on the assessment models and covers the following main areas of data protection: processing and lawfulness basis of data use, data quality, rights of data subjects, data transfer, data processors and personnel authorised to access information, data security, and risk management.

SECTION 1. PROCESSING AND LAWFULNESS BASIS

- ✓ Does the project involve the collection of information about individuals?

- If no, the survey is finished.

✓ Are data subjects compelled to provide information about themselves?

✓ Is a freely given, specific, informed and unambiguous consent of data subjects required in order to proceed with the processing?

- If no, which is the legal basis of the processing?
  - Is the processing necessary in relation to a contractual relationship with the data subject?
  - Is the processing required or authorised by law?
  - Is the processing necessary in order to protect a vital interest of the data subjects?
  - Is the processing necessary for the performance of a task carried out in the public interest?
  - Is the processing necessary for the satisfaction of the legitimate interest of the controller?

✓ What kind of information is to be collected? (In particular, specify if special categories of data[168] are processed)

✓ Which are the purposes of the processing?

✓ Which means are used for the processing (e.g. electronic means, non-automated means)?

✓ Are new technologies used which might be perceived as being privacy intrusive (e.g. facial recognition, use of biometrics)?

✓ At the moment of the data collection, is a concise, transparent, intelligible and clear notice[169] and consent given to the data subjects?

✓ Are provided procedures for the withdrawal of the consent?

✓ Is information about data subjects disclosed to organisations or people?

- If yes, to whom?

SECTION 2. QUALITY OF THE COLLECTED INFORMATION

✓ Is the collected information necessary in relation to the purposes for which they are processed?

✓ Is the collected information used for different or incompatible purposes than those established and communicated to data subjects?

✓ Do exist procedures to verify and ensure the accuracy and the update of collected information?

[168] Special categories of data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[169] In a complete notice and consent form, purposes and means of the processing shall be explained and contact details of the controller and the DPO (if present), authorised subjects to access information, period of storage and data subjects' rights shall be outlined.

- ✓ Is the information of data subjects stored by the controller?
    - If no, skip to section 3.
- ✓ For how long is information stored?
- ✓ Is information stored in a way which allows the exercise of data subjects' rights?
- ✓ Which storage mechanisms/procedures are provided? (centralized databases, archives, smart card, and so on)
- ✓ Is there a records management policy in place which includes a retention and destruction schedule?
- ✓ If information is converted in anonymous information, are there procedures which ensure the irreversibility of the process and the impossibility to re-identify data subjects?

SECTION 3. RIGHTS OF DATA SUBJECTS

- ✓ Are there free of charge and simple modalities for the exercise of the rights of the data subject?
- ✓ Does the controller adopt measures to verify the identity of the data subject who exercises rights?
- ✓ Are there adequate measures or procedures which ensure the reply to every request of data subjects?
- ✓ Might data subjects have the opportunity to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed?
- ✓ Might data subjects have access to the information which refers to them?
- ✓ Might data subjects have the opportunity to obtain the rectification of any erroneous information about them?
- ✓ Might data subjects have the opportunity to obtain from the controller restriction of processing?
- ✓ Might data subjects have the opportunity to obtain from the controller the erasure of personal data concerning him or her without undue delay?
- ✓ Are there procedures to communicate any rectification, erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed?
- ✓ If requested, is information provided by the controller in a structured, commonly used and machine-readable format?
- ✓ Might data subjects have the opportunity to transmit those data to another controller without hindrance from the controller to which the personal data have been provided?
- ✓ If decisions are based solely on automated processing, including profiling, which produces legal effects concerning, might data subjects refuse to be subject to this kind of decision?

- ✓ Are there procedures which allow data subjects to know the evaluation criteria of the automated individual decision-making?

SECTION 4. TRANSFER

- ✓ Are personal data transferred outside of the European Union?
- ✓ Will personal data be transferred outside of the European Union?
    - o If no, skip to section 5.
- ✓ Is there an adequacy decision in relation to the third State importer of personal data?
    - o If no, skip to section 5.
- ✓ Are there appropriate safeguards in relation to the third State importer of personal data?
    - o If no, skip to section 5.
- ✓ In the absence of an adequacy decision or of appropriate safeguards, which is the basis of lawfulness for the transfer?
    - The data subject has explicitly consented
    - The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
    - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
    - The transfer is necessary for important reasons of public interest
    - The transfer is necessary for the establishment, exercise or defence of legal claims
    - The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
    - The transfer is made from a public register

SECTION 5. PROCESSORS AND PERSONNEL AUTHORISED TO ACCESS INFORMATION

- ✓ Is the relationship between controller and processor regulated by mean of a contract or other legal act?
- ✓ Are the instructions to the processor outlined?
- ✓ Might the processor engage another processor under the prior authorisation of the controller?

SECTION 6. SECURITY

- ✓ Is a data protection officer or an information security officer appointed?

- ✓ Does the controller implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation?
- ✓ Does the controller implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed?
- ✓ Has the controller outlined functions and obligations of personnel authorised to access to IT systems where personal data are stored?
- ✓ Does the controller ensure that the personnel is aware of the adopted security measures?
- ✓ Does the controller ensure that every authorised person can access only to personal data which are necessary to carry out his functions?
- ✓ Does the controller assign to his personnel a specific and unique account which ensure the certain identification and authentication of the authorised person?
- ✓ Is there an access register to the IT systems containing personal data?
    - o For how long is the access register stored?
    - o Do procedures exist which allow the DPO or the IT security officer periodically to check the access register?
- ✓ Are there procedures or mechanisms to create backups?
- ✓ Does the controller periodically verify the proper functioning of security procedures and measures?
- ✓ Are there controls of physical access to the places where personal data are stored?
- ✓ Are administrative, technical and physical safeguards in place to protect information against theft, loss, unauthorised access, use or disclosure and unauthorised copying, modification or disposal? (Administrative measures are for example rules and procedures which regulate the organizational aspects of security; technical safeguards mean encryption and pseudonymisation techniques, disaster recovery plans, backups, operational continuity plans; physical measures are like locks, reinforced doors, window bars)
- ✓ Is there a data breach management action plan in place?
- ✓ Did the controller, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data?
    - o Did the data protection impact assessment indicate that the processing would have resulted in a high risk in the absence of measures taken by the controller to mitigate the risk?
    - o Since the high risk indicated by the data protection impact assessment, did the controller consult the supervisory authority prior to processing?
    - o Will the controller carry out a data protection impact assessment?
- ✓ Does the controller join code of conducts or adopt certification mechanisms?
- ✓ Does the controller adopt data protection seals and marks?

SECTION 7. RISKS MANAGEMENT

- ✓ Does the technology allow to perform evaluation or scoring of the data subjects?
- ✓ Does the technology allow the collected data to be easily matched or combined with other data sets?
- ✓ Does the technology allow the collection of personal data on a large scale?
- ✓ Does the technology allow the collection of personal data in contexts that are private (such as devices specifically designed to be used in private houses) or that refer to private situations (such as devices that could register private conversations)?
- ✓ Does the technology allow for the collection of sensitive personal data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health, sex life or sexual orientation) or data relating to criminal convictions and offences?
- ✓ Does the technology allow for the collection of personal data whose leak could risk damaging the data subject (e.g. financial data that could be used for payment frauds)?
- ✓ Does the technology allow the collection of personal data referring to vulnerable subjects (e.g. of patients in hospitals, of employees in the working environment, of children)?
- ✓ Does the technology allow to observe, monitor or control data subjects in a systematic way?
- ✓ Does such control take place in a publicly accessible area?
- ✓ Does the technology allow the data subjects to be aware of the monitoring in process?
- ✓ Is the data subject able to avoid such monitoring and control?
- ✓ Does the technology allow (full or partial) automated-decisions to be taken with regard to the data subjects?
- ✓ Do such decisions affect legal rights of the data subjects (for instance, if the data collected by the device allows to detect alleged non-performance of the data subject and therefore prevents the device to work properly)?
- ✓ Do such decisions similarly significantly affect the natural person (for instance, if the collected data can be used to deny the data subject access to essential services, such as health, education or financial services)?
- ✓ Does the technology allow for human intervention in the decision process?
    - If yes, is such human intervention enough to prevent risks to the rights of the data subjects?
- ✓ Is the technology that I am developing new in terms of the potential impact on data subjects?

- ✓ Am I using a product/component developed by others who have already carried out a DPIA?
    - If yes, check whether the producer is willing to share the DPIA and integrate such a DPIA in your own assessment.
- ✓ Am I developing a technology similar to others that are being developed?
    - If yes, consider the possibility to carry out a joint DPIA.
- ✓ Are there codes of conduct that could be taken into account?
- ✓ Have I clearly identified the nature, scope, context and purposes of the processing operations?
- ✓ Have I identified the assets on which the personal data rely (e.g. hardware, software, people, paper…)?
- ✓ Have I consulted all the subjects that are involved in the processing operations (e.g. the DPO, the processors)?
- ✓ Is it feasible to consult the data subjects or their representatives on the impact of the technology on their rights and interests? If yes, have I done so?
- ✓ Have I envisaged measures to restrict the collection and further processing and storage of data to what is strictly necessary for the purposes of the processing?
- ✓ Does the technology makes it possible to provide the data subject with all the necessary information regarding the processing?
- ✓ Does the technology allow the collected data to be modified and erased?
- ✓ Have I clearly identified the risks to the rights and freedoms of natural persons?
- ✓ Have I assessed the severity of such risks?
- ✓ Have I assessed the likelihood of such risks?
- ✓ Have I identified specific measures for each of the assessed risks?
- ✓ Have I identified measures to mitigate risks of illegitimate access, modification or disappearance of the data collected by the devices?
- ✓ Is it possible to publish the DPIA partially or in a summarised way without hindering the rights of the technology developers or of the data subjects?
- ✓ Are the measures that I have designed sufficient to mitigate the risks to the rights and freedoms of the data subjects? If the answer is no, have I consulted the national supervisory authority?

II.3.2.2 The Ethical and Social sections

The provision of a complete PESIA model, which includes the sections focused on ethical and societal issues, is the main goal of D4.4. This deliverable (D4.3) provides “some initial guidelines” for the adoption of PESIA. These guidelines represent the

result of the research activities carried out in the first part of Task 4.3 (M15-M27) and Task 4.4 (M18-M27), which are focuses on the development of guidelines and the questionnaires to be used by developers for a self-assessment of the privacy, ethical and social impacts of their products or services.

The complete structure of PESIA model as well as its sector-specific applications, which characterise the last part of the activities outlined in Tasks 4.3. and 4.4 are still under development and the outcome of the ongoing research will be described in the next deliverable (D4.4). In this light, Deliverable 4.3 provides a first draft of these sections which is more focused on the legal values, formulating specific questions for each main area and providing some cases. Questions and cases will be then further tested and implemented with a focus on the societal values in the following months through the interaction with developers and their communities and on the basis of the ethnographic ongoing research.

As mentioned above, the PESIA structure – mainly with regard to the sections devoted to ethical and social issues – is based on a list of questions, focused on the different values, and some case that can facilitate users in the understanding the main issue addressed by these questions. The following tables outlines this approach in six different value fields: accountably, dignity, non-discrimination, autonomy, transparency, and participation.

Accountability	
Case	*A company is developing a connected doll which, to reduce its cost, will be sponsored by other companies. These sponsors cover part of the production costs and obtain that the doll provides users some advertising messages about their products.*
Questions	✓ Have you developed a process to identify and consider ethical and social issues related to your product/service? ✓ Have you considered data protection issues since the beginning of product /service development? ✓ Have you considered ethical and social issues since the beginning of product /service development? ✓ Have you adopted any specific measures to assess and mitigate the potential privacy, ethical and social consequences of the product/service throughout its entire life-circle?

Dignity	
Case (example)	*A company adopts an IoT-based technology to improve work productivity. All employees receive a wearable IoT device (an electronic bracelet) equipped with a GPS*

	technology able to monitor their movements within the working spaces, including the restrooms, in order to better monitor and manage the production cycle.
Questions	✓ Considering data processing and its purposes, may your IoT application have any impact on human dignity? ✓ Does the IoT device need to be implanted into the user's body? ✓ Is the IoT device able to transmit sensations to the user's body (e.g. vibrations, sounds, etc.)? ✓ Could the device interfere or limit the normal functionality of the user's body (e.g. exoskeletons)?

Non-discrimination	
Case	*A company decides to produce wearable devices that can be used to monitor health conditions. The devices are wristwatches that can gather information about the number of steps walked, user's heartbeat, her blood pressure, and other personal data concerning fitness training. The collected data can be shared with private insurance companies, credit companies and employment agencies.*
Questions	✓ Are the IoT device and associated software used for predictive purposes or classifying users according to their conditions, behaviour and preferences? ✓ May the IoT application create forms of discrimination against the users or third parties? ✓ Are the services associated to the IoT devices provided in a manner that may create forms of unfair discrimination?

Autonomy	
Case	*A company is developing a smart transport system that improves traffic management and driving safety. The system requires the installation of an IoT device inside each vehicle to collect data on vehicle position, driving styles, speed and other users' behaviours. The data collected can be shared with roadside assistance services, insurance companies and other third parties.*
Questions	✓ May the use of the IoT device limit individual autonomy (e.g. remote control)? ✓ If these limitations exist, do they happen in contexts characterised by power asymmetries (e.g.

	workplace)?

Transparency	
Case	*A municipality decides to adopt IoT technology to find people in the crowd (e.g. in the event of health emergency) during concerts or other large-scale events organised in the local stadium. A wearable IoT device is provided to all participants in these events. The collected data can be shared with the private companies that organise these events, public health services and local police department.*
Questions	✓ Has any information been provided about the project to the interested persons or to the public at large? ✓ Has the project adopted any procedure to give the opportunity to persons to ask information about the project? ✓ Has information about the logic of data processing been provided to data subjects?

Participation	
Case	*A regional transportation authority develops a new multimodal service that gives passengers the opportunity to use different transportation services with the same personal IoT-based smart card. The regional system can potentially collect an extensive amount of mobility data concerning passengers and share them with transportation service providers and third parties.*
Questions	✓ Have you planned to engage stakeholders in the project development? ✓ In which manner have you identified the relevant stakeholders? ✓ Which forms of engagement of the stakeholders have you adopted? ✓ Which kind of information about the project and data processing have been disclosed to the stakeholders? ✓ Do you intend to implement the suggestions provided by the stakeholders? Do you plan to present to the stakeholders this implementation for a further discussion? ✓ Have you considered to provide publicly available information about this consultation?

Annexes

I. List of the PIA/DPIA models

European Union

- Belgium, “Projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique (CO-AR-2016-004)”, Commission de la Protection de la Vie Privée, 2016
- Catalunya, “Avaluació d’impacte relativa a la protecció de dades”, Autoritat Catalana de Protecció de Dades for Catalunya, June 2017
- France, “PIA Methodology” - “PIA Tools” -“PIA Good Practices”, Commission Nationale de l’Informatique et des Libertés (CNIL), June 2015
- Germany, “The Standard Data Protection Model. A concept for inspection and consultation on the basis of unified protection goals”, V. 1.0 – Trial Version, Conference of the German Independent Data Protection Authorities of the Bund and the Länder, 9-10 November 2016
- Ireland, “Guidance on Privacy Impact Assessment in Health and Social Care”, Health Information and Quality Authority, December 2010
- Netherlands, “Privacy Impact Assessment (PIA) Introductie, handreiking en vragenlijst”, Vers. 1.2, Dutch Data Protection Authority with NOREA, last update on November 2015
- Spain, “Guìa para la Evaluación de Impacto en la Protección de Datos Personales (EIPD)”, Agencia Española de Protección de Datos for Spain, 2014
- United Kingdom: “Conducting privacy impact assessments Code of practice”, Information Commissioner’s Office, February 2014

Third countries

- Australia, “Guide to undertaking privacy impact assessments”, Office of the Australian Information Commissioner (OAIC), May 2014
- Canada (British Columbia), “Privacy Impact Assessment Guidelines”, Privacy and Legislation Branch - Office of the Chief Information Officer, May 2014
- Canada (Federal Government), “A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada”, Office of the Privacy Commissioner of Canada, 2011
- Canada (Ontario), “Planning for Success: Privacy Impact Assessment Guide”, Office of the Information and Privacy Commissioner, May 2015
- Hong Kong, “Information Leaflet on PIAs”, Office of the Privacy Commissioner, October 2015
- New Zealand, “PIA Toolkit”, Office of the Privacy Commissioner, 2015

II. List of ECtHR and ECJ decisions

- ECJ, C-101/01, Lindquist, 6 November 2003
- ECJ, C-201/14, Smaranda Bara et al. v. Presedintele Casei Nationale de Asigurari de Sanatate (CNAS) et al., 1.10.2015
- ECJ, C-342-12, Worten – Equipamento para o Lar SA v. ACT (Authority for Working Conditions, 30.5.2013
- ECJ, C-362/14, Schrems v. Data protection Commissioner, 6.10.2015
- ECJ, C-524/06, Huber v. Germany, 16.12.2008
- ECJ, C-553/07, College Van Burgemeester En Wethouders Van Rotterdam v. Rijkeboer, 7.5.2009
- ECJ, C-615/13 P. Client Earth et at. v. EFSA, 16.7.2015
- ECJ, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy and Satamedia, 16 December 2008
- ECJ, C-92/09, Volker und Markus Schecke GBR v. Land Hessen
- ECJ, C-93/09, Eifert v. Land Hessen and Bundesanstalt fur Landwirtschaft und Ernahrung, 9 November 2010
- ECJ, C 131/12, Google Spain SL v. AEDP and Mario Costeja, 13 May 2014
- ECJ, C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 11 December 2014
- ECJ, C-291/12, Michael Schwarz v. Stadt Bochum, 17 October 2014
- ECJ, T-320/02, Esch-Leonhardt and others v. European Central Bank, 18.2.2004
- ECtHR, A. v. the United Kingdom, 17 July 2003
- ECtHR, Alkaya v. Turkey, judgment of 9 October 2012
- ECtHR, Allan v. the United Kingdom, 5 November 2002
- ECtHR, Amann v. Switzerland, 16 February 2000
- ECtHR, Anne-Marie Andersson v. Sweden, 27 August 1997
- ECtHR, Annen v. Germany, 26 November 2015
- ECtHR, Antović and Mirković v. Montenegro, 28 November 2017
- ECtHR, Association “21 Décembre 1989” and Others v. Romania, 24 May 2011
- ECtHR, Avram and Others v. Moldova, 5 July 2011
- ECtHR, Axel Springer AG v. Germany, 7 February 2012
- ECtHR, B.B. v. France, Gardel v. France, M.B. v. France, 17 December 2009
- ECtHR, Bărbulescu v. Romania, 5 September 2017
- ECtHR, Biriuk v. Lithuania, 25 November 2008
- ECtHR, Brunet v. France, 18 September 2014
- ECtHR, Cemalettin Canlı v. Turkey, 18 November 2008

- ECtHR, Copland v. United Kingdom, 3 April 2007
- ECtHR, Cotlet v. Romania, 3 June 2003
- ECtHR, Dalea v. France, 2 February 2010
- ECtHR, Dragojević v. Croatia, 15 January 2015
- ECtHR, Flinkkilä and Others v. Finland, 6 April 2010
- ECtHR, Gaskin v. The United Kingdom, 7 July 1989
- ECtHR, Gillberg v. Sweden, 3 April 2012
- ECtHR, Godelli v. Italy, 25 September 2012
- ECtHR, Halford v. The United Kingdom, 25 June 1997
- ECtHR, Haralambie v. Romania, 27 October 2009
- ECtHR, HR, Bykov v. Russia, 10 March 2009
- ECtHR, HR, Uzun v. Germany, 2 September 2010
- ECtHR, HR, Z. v. Finland, 25 February 1997
- ECtHR, I. v. Finland, 17 July 2008
- ECtHR, I. v. Finland, 3 April 2007
- ECtHR, Iordachi and others v. Moldova, 14 September 2009
- ECtHR, K.H. and others v. Slovakia, 28 April 2009
- ECtHR, K.U. v. Finland, 2 December 2008
- ECtHR, Kennedy v. The United Kingdom, 18 May 2010
- ECtHR, Khelili v. Switzerland, 18 October 2011
- ECtHR, Khmel v. Russia, 12 December 2013
- ECtHR, Kinnunen v. Finland, 15 May 1996
- ECtHR, Klass and others v. Germany, 6 September 1978
- ECtHR, Köpke v. Germany, 5 October 2010
- ECtHR, Kruslin v. France, 24 April 1990
- ECtHR, Kurier Zeitungsverlag und Druckerei GmbH v. Austria (No. 2), 19 June 2012
- ECtHR, L.L. v. France, 10 October 2006
- ECtHR, Lambert v. France, 24 August 1998
- ECtHR, Leander v. Sweden, 26 March 1987
- ECtHR, Liberty and others v. United Kingdom, 1 July 2008
- ECtHR, López Ribalda and others v. Spain, 9 January 2018
- ECtHR, M.G v. the United Kingdom, 24 September 2002
- ECtHR, M.K. v. France, 18 April 2013
- ECtHR, M.K. v. France, 18 April 2013

- ECtHR, M.M. v. the United Kingdom, 13 November 2012
- ECtHR, M.N. v. San Marino, 7 July 2015
- ECtHR, M.S. v. Sweden, 27 August 1997
- ECtHR, Malone v. The United Kingdom, 2 August 1984
- ECtHR, Matheron v. France, 29 March 2005
- ECtHR, Matwiejczuk v. Poland, 2 December 2003
- ECtHR, McMichael v. The United Kingdom, 24 February 1995
- ECtHR, McVeigh, O'Neill and Evans v. the United Kingdom, 18 March 1981
- ECtHR, Mikolajová v. Slovakia, 18 January 2011
- ECtHR, Mitkus v. Latvia, 2 October 2012
- ECtHR, Mosley v. the United Kingdom, 10 May 2011
- ECtHR, Nada v. Switzerland, 12 September 2012
- ECtHR, Niemietz v. Germany, judgment of 16 December 1992
- ECtHR, Odièvre v. France, 13 February 2003
- ECtHR, P. and S. v. Poland, 30 October 2012
- ECtHR, P.G. and J.H. v. the United Kingdom ,25 September 2001
- ECtHR, Peck v. the United Kingdom, 28 January 2003
- ECtHR, Perrin v. The United Kingdom, 18 October 2005
- ECtHR, Peruzzo and Martens v. Germany, 4 June 2013
- ECtHR, Pisk-Piskowski v. Poland, 14 January 2005
- ECtHR, Pruteanu v. Romania, 3 February 2015
- ECtHR, R.E. v. United Kingdom, 27 October 2015
- ECtHR, Roman Zakharov v. Russia, 4 December 2015
- ECtHR, Rotaru v. Romania, 4 May 2000
- ECtHR, S. and Marper v. the United Kingdom, 4 December 2008
- ECtHR, Saaristo and Others v. Finland, 12 October 2010
- ECtHR, Satamedia v. Finland, 21 July 2015
- ECtHR, Sciacca v. Italy, 11 January 2005
- ECtHR, Segerstedt-Wiberg and Others v. Sweden, 6 June 2006
- ECtHR, Shimovolos v. Russia, 21 June 2011
- ECtHR, Szabó and Vissy v. Hungary, 12 January 2016
- ECtHR, Szuluk v. The United Kingdom, 2 June 2009
- ECtHR, Taylor-Sabori v. the United Kingdom, 22 October 2002
- ECtHR, Turek v. Slovakia, 14 February 2006
- ECtHR, Van der Velden v. the Netherlands, 2006

- ECtHR, Verlagsgruppe News GmbH and Bobi v. Austria, 4 December 2012
- ECtHR, Vetter v. France, 31 May 2005
- ECtHR, Von Hannover v. Germany, 24 June 2004
- ECtHR, Wisse v. France, 20 December 2005
- ECtHR, Yuditskaya and Others v. Russia, 12 February 2015
- ECtHR, Z. v. Finland, 25 February 1997
- ECtHR, Zaichenko v. Ukraine, 26 February 2015

III. List of the decisions adopted by DPAs

A. Belgium

- Commission de la protection de la vie privée, n. 18/2013, 5 June 2013;
- *Commission de la protection de la vie privée*, recommandation n. 03/2013, 24 April 2013;
- Commission de la protection de la vie privée, recommandation n. 8/2012, 2 May 2012;
- Commission de la protection de la vie privée, recommandation n. 05/2010 , 15 December 2010;
- Commission de la protection de la vie privée, recommandation n. 01/2010, 17 March 2010;
- Commission de la protection de la vie privée, avis n. 27/2009, 28 October 2009;
- Commission de la protection de la vie privée, recommandation n. 01/2009, 18 March 2009;
- Commission de la protection de la vie privée, avis n. 17/2008, 9 April 2008;
- Commission de la protection de la vie privée, avis, n. 8/2006, 12 April 2006;
- *Commission de la protection de la vie privée*, n. 12/2005, 7 September 2005;
- Commission de la protection de la vie privée, avis n. 39/2001, 8 October 2001;
- Commission de la protection de la vie privée, avis n. 10/2000, 3 April 2000;
- Commission de la protection de la vie privée, avis n. 10/2000, 3 April 2000;
- Commission de la protection de la vie privée, Faq *"La géolocalisation"* https://www.privacycommission.be/fr/la-geolocalisation;
- Commission de la protection de la vie privée, FAQ, *https://www.privacycommission.be/fr/collecte-de-donnees-du-candidat-aupres-du-precedent-employeur-et-de-ses-clients-lenquete-de*;

B. France

- Commission Nationale de l'Informatique et des Libertés, n. 2017-009, 15 June 2017;
- Commission Nationale de l'Informatique et des Libertés, n. 2016-221, 21 July 2016;
- Commission Nationale de l'Informatique et des Libertés, n. 2016-220, 21 July 2016;
- Commission Nationale de l'informatique et des libertés: n. 2016-017, 28 January 2016;
- Commission Nationale de l'Informatique et des Libertés, n. 2015-088, 5 March 2015;

- Commission Nationale de l'Informatique et des Libertés, n. 2014-307, 17 July 2014;
- Commission Nationale de l'Informatique et des Libertés, n. 2014-294, 22 July 2014;
- Commission Nationale de l'Informatique ed des Libertés, n. 2013-366, 23 November 2013;
- Commission Nationale de l'Informatique et des Libertés, n. 2013-029, 13 July 2013;
- Commission Nationale de l'Informatique et des Libertés, n. 2013-139, 30 May 2013;
- Commission Nationale de l'Informatique et des Libertés, n. 2010-112, 22 April 2010;
- Commission Nationale de l'Informatique et des Libertés, n. 2010-096, 8 April 2010;
- Commission Nationale de l'Informatique et des Libertés, n. 2009-201, 16 April 2009;
- Commission Nationale de l'Informatique et des Libértes, n. 2009-002, 20 January 2009;
- Commission Nationale de l'Informatique et des Libertés, n. 2008-492, 11 December 2008;
- Commission Nationale de l'Informatique et des Libertés, n. 2006-066, 16 March 2006;
- Commission Nationale de l'Informatique et des Libertés, n. 94-056, 21 June 1994;

C. Germany

- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/BeschaeftigungArbeitArtikel/Videoüberwachung.html*.
- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/DVSystemeArbeitsplatzArtikel/InternetnutzungArbeitsplatz.html.
- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/BeschaeftigungArbeitArtikel/Mitarbeiterbefragungen.html*.
- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/PersonalArbeitnehmerdatenArtikel/NotenspiegelImInternet.html*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, National Konferenz 30th March 2017: *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/DSK_Entschliessung_Gesichtserkennung.html?nn=5217228*.

- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, National Konferenz 23th March 2017, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/DSK_EntschliessungGesetzentwurfAufzeichnungFahrdaten.html?nn=5217228*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, National Konferenz 16th January 2017, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/PassAuswGSonder_DSKFassung.html?nn=5217228*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 92nd National Konferenz 9th November 2016: *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/92DSK_Videoueberwachungsverbesserungsgesetz.html?nn=5217228*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 91st National Konferenz 6th-7th April 2016, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91DSK_EntschliessungWearables.html?nn=5217228.Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 89th National Konferenz 18th-19th March 2015, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-DatenschutzNachCharlyHebdo.html?nn=5217228.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 89th National Konferenz 18th-19th March 2015, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-VerschluesselungOhneEinschraenkungenErmoeglichen.html?nn=5217228*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 89th National Konferenz 18th-19th March 2015, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-BigData.html?nn=5217228*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, National Konferenz 14th November 2014, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/14112014_EntschliessungPKWMaut.html?nn=5217228*.
- Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 88th National Konferenz 8th-9th October 2014, *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_DatenschutzImKfz.html?nn=5217228*.

D. Italy

- Garante per la protezione dei dati personali, 1 febbraio 2018, doc. web n. 8159221;
- Garante per la protezione dei dati personali, 21 dicembre 2017; doc. web n. 7496252;

- Garante per la protezione dei dati personali, 24 novembre 2016, n, 488, doc. web n. 5796783;
- Garante per la protezione dei dati personali 27 ottobre 2016 n. 439, doc. web n. 5687770;
- Garante per la protezione dei dati personali, 6 ottobre 2016, n. 389, doc. web n. 5508051;
- Garante per la protezione dei dati personali, 8 settembre 2016, n. 350, doc. web n. 5497522;
- Garante per la protezione dei dati personali 18 giugno 2015, n. 360, doc. web n. 4170232.
- Garante per la protezione dei dati personali 4 giugno 2015, n. 345, doc. web n. 4211000;
- Garante per la protezione dei dati personali 28 maggio 2015 n. 319, doc. web n. 4131145.
- Garante per la protezione dei dati personali, 7 novembre 2013, n. 499, doc. web n. 2911484;
- Garante per la protezione dei dati personali, 30 ottobre 2013, n. 483, doc. web n. 2851973;
- Garante per la protezione dei dati personali, 30 ottobre 2013, n. 484, doc. web n. 2908871;
- Garante per la protezione dei dati personali, 5 settembre 2013, n. 385, doc. web n. 2683203;
- Garante per la protezione dei dati personali, 1 agosto 2013, n. 384, doc. web n. 2578547;
- Garante per la protezione dei dati personali, 4 luglio 2013, n. 335, doc. web n. 2577227;
- Garante per la protezione dei dati personali, 8 maggio 2013 n. 230, doc. web n. 2433401;
- Garante per la protezione dei dati personali, 4 aprile 2013, n. 164, doc. web n. 2439178;
- Garante per la protezione dei dati personali 7 marzo 2013, n. 103, doc. web n. 2471134;
- Garante per la protezione dei dati personali 24 febbraio 2010, doc. web n. 1705070;
- Garante per la protezione dei dati personali, 10 luglio 2008, doc. web n. 1536583;
- Garante per la protezione dei dati personali, 8 marzo 2007, doc. web n. 1391803.
- Garante per la protezione dei dati personali, 11 gennaio 2007, doc. web n. 1381620;
- Garante per la protezione dei dati personali, 15 giugno 2006, n. 1306098;

- Garante per la protezione dei dati personali, 21 luglio 2005, doc. web 1150679;
- Garante per la protezione dei dati personali, 9 marzo 2005, doc. web n. 1109493;
- Garante per la protezione dei dati personali, 11 dicembre 2000, doc. web n. 30903;
- Garante per la protezione dei dati personali, 8 giugno 1999, doc. web n. 40369.
- Garante per la protezione dei dati personali, 12 ottobre 1998, doc. web n. 1109147.

E. Spain

- Agencia Española de Protección de Datos, Expediente n. 01769/2017;
- Agencia Española de Protección de Datos, Expediente n. 01760/2017;
- Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017;
- Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0065/2015;
- Agencia Española de Protección de Datos, Resolución R/01208/2014;
- Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0464/2013;
- Agencia Española de Protección de Datos, Expediente n. E/02689/2012;
- Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0392/2011;
- Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0292/2010;
- Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 368/2006;

F. United Kingdom

- Information Commissioner's Office, *CCTV – Public advice*;
- Ico. Information Commissioner's Office, *Wi-fi location analytics*;
- Ico. Information Commissioner's Office*, The use of biometrics in schools*;
- Ico. Information Commissioner's Office, *The employment Practices. Code Supplementary Guidance;*
- Ico. Information Commissioner's Office, *The employment practices code;*
- Ico. Information Commissioner's Office, *Quick guide to the employment practices code Ideal for the small business*;
- Ico. Information Commissioner's Office, *Publication of exam results by schools*;
- Ico. Information Commissioner's Office, *Privacy in mobile apps. Guidance for app developers*;
- Ico. Information Commissioner's Office*, In the picture: A data protection code of practice for surveillance cameras and personal information*;

- Ico. Information Commissioner's Office*, ICO view on CCTV installation being made a condition of an alcohol licence by the licensing authority*;
- Ico. Information Commissioner's Office, *Guide to the Privacy and Electronic Communications Regulations*;
- Ico. Information Commissioner's Office, *Drones*;
- Ico. Information Commissioner's Office, *Data Protection Technical Guidance Radio Frequency Identification*;
- Ico. Information Commissioner's Office, *Data protection and journalism: a guide for the media*;
- Ico. Information Commissioner's Office, *Big data, artificial intelligence, machine learning and data protection*;

G. Article 29 Data Protection Working Party

- Article 29 Data Protection Working Party, WP 252, *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)*, adopted on 4 October 2017;
- Article 29 Data Protection Working Party, WP 223, *Opinion 8/2014 on the on Recent Developments on the Internet of Things,* adopted on 16 September 2014;
- Article 29 Data Protection Working Party, WP 215, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, adopted on 10 April 2014;
- Article 29 Data Protection Working Party, *Letter addressed to Google regarding Google Glass, a type of wearable computing in the form of glasses,* 18 June 2013;
- Article 29 Data Protection Working Party, WP193, *Opinion 3/2012 on developments in biometric technologies,* adopted on 27 April 2012;
- Article 29 Data Protection Working Party, WP 205*, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force,* adopted on 22 April 2013;
- Article 29 Data Protection Working Party, WP 185, *Opinion 13/2011 on Geolocation services on smart mobile devices,* adopted on 16 May 2011;
- Article 29 Data Protection Working Party, WP 181, *Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime,* adopted on 5 April 2011;
- Article 29 Data Protection Working Party, WP 183, *Opinion 12/2011 on smart metering*, adopted on 4 April 2011;
- Article 29 Data Protection Working Party, WP 180, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications,* adopted on 11 February 2011;

- Article 29 Data Protection Working Party, WP175, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications,* adopted on 13 July 2010;
- Article 29 Data Protection Working Party, WP 147, *Working Document on the protection of children's personal data (General guidelines and the special case of school),* adopted on 18 February 2008;
- Article 29 Data Protection Working Party, WP134*, Opinion n. 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006)269 final),* adopted on 1 March 2007;
- Article 29 Data Protection Working Party, WP 125*, Working document on data protection and privacy implications in eCall initiative,* adopted on 26 September 2006;
- Article 29 Data Protection Working Party*, WP 115 Working Party 29 Opinion on the use of location data with a view to providing value-added services*, adopted on 25 November 2005;
- Article 29 Data Protection Working Party, WP 113, *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005*), adopted on 21 October 2005;

- Article 29 Data Protection Working Party, WP105*, Working document on data protection issues related to RFID technology*, adopted on January 19, 2005;
- Article 29 Data Protection Working Party, WP 96*, Opinion n. 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS),* adopted on 11 August 2004;
- Article 29 Data Protection Working Party, WP 89, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance,* adopted on 11 February 2004;
- Article 29 Data Protection Working Party, WP 80, *Working document on biometrics,* adopted on 1 August 2003;
- Article 29 Data Protection Working Party, WP 67, *Working Document on the Processing of Personal Data by means of Video Surveillance*, adopted on 25 November 2002;
- Article 29 Data Protection Working Party, WP 55,*Working document on the surveillance of electronic communications in the workplace*, adopted on 29 May 2002;
- Article 29 Data Protection Working Party, WP 48*, Opinion 8/2001 on the processing of personal data in the employment context*, adopted on 13 September 2001;

IV. Main references

- Article 29 Data Protection Working Party. 2014. Statement on the role of a risk-based approach in data protection legal frameworks.
- Article 29 Data Protection Working Party. 2016. Guidelines on Data Protection Officers ('DPOs').
- Article 29 Data Protection Working Party. 2017. Guidelines for identifying a controller or processor's lead supervisory authority.
- Article 29 Data Protection Working Party. 2017. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, revised and adopted on 4 October 2017.
- Article 29 Data Protection Working Party. 2017. Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, last revised and adopted on 5 April 2017.
- Article 29 Data Protection Working Party. 2017. Guidelines on the right to data portability, adopted on 13 December 2016, last revised and adopted on 5 April 2017.
- Article 29 Data Protection Working Party. 2018. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/677, adopted on 3 October 2017, as last revised and adopted on 6 February 2018.
- Article 29 Data Protection Working Party. 2018. Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, last revised and adopted on 11 April 2018.
- Asveld L. and Roeser S. (eds.). 2009. The Ethics of Technological Risk (London, Sterling, VA : Earthscan).
- Barocas S., Selbst A. D. 2016. Big Data's Disparate Impact. 104 (3) California Law Rev. 671-732.
- Bygrave L. A. 2004, Privacy Protection in a Global Context – A Comparative Overview. 47 Scandinavian Studies in Law 319–348.
- Cate F. H. 2008. Government Data Mining: The Need for a Legal Framework. 43 (2) Harvard Civil Rights-Civil Liberties Law Review 435-489.
- Clarke R. 2014. The regulation of civilian drones' impacts on behavioural privacy. 30 (3) Comp. Law & Sec. Rev. 286-305.
- Council of Europe. 2017. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a.
- Custers B., Calders T., Schermer B., Zarsky T. (eds.). 2013. Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, (Berlin, Heidelberg : Springer Berlin Heidelberg).

- Daniel S.J. 2006. A Taxonomy of Privacy. 154(3) Penn. Law. Rev. 477–560.
- De Hert, P. 1997. Human Rights and Data Protection. European CaseLaw 1995–1997 [Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955–1997]. In Jaarboek ICM 1997 (Antwerpen, Maklu, 1998).
- Eberle E.J. 2002. The Right to Information Self-Determination. 2001 Utah L. Rev. 965-995.
- Federal Trade Commission. 2007. Credit-Based Insurance Scores: Impacts on consumers of automobile insurance, Report to Congress. https://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta_report_credit-based_insurance_scores.pdf.
- Fialova E. 2014. Data Portability and Informational Self-Determination. 8(1) Masaryk U. J.L. & Tech. 45-55.
- Fritsch, E., Shklovski, I., and Douglas-Jones, R. 2018. Calling for a revolution: An analysis of IoT manifestos. In Proceedings of the 2018 ACM Conference on Human Factors in Computing (Montreal, Canada).
- Mantelero A., Data protection, e-ticketing, and intelligent systems for public transport, (2015), V, 4, 309, Int. Data Privacy Law.
- Mantelero A. 2016. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. 32(2) Comp. Law and Sec. Rev. 238-255.
- Mantelero A., Vaciago G. 2013. The “Dark Side” of Big Data: Private and Public Interaction in Social Surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds. 14(6) Comp. Law Rev. Int. 161-169.
- Mayer-Schönberger V., Cukier K. 2013. Big Data: A Revolution That Will Transform How We Live, Work, and Think (London : John Murray).
- Merry S. E. 2013. McGill Convocation Address: Legal Pluralism in Practice. 59 (1) McGill Law Journal 1–8.
- Montgomery K., Chester J., Kopp K. 2018. Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment. 8 Journal Inf. Pol. 34-77.
- Nissenbaum H. 2010. Privacy in Context. Technology, Policy and the Integrity of Social Life (Stanford : Stanford University Press).
- Penney J.W. 2016. Chilling Effects: Online Surveillance and Wikipedia Use. 31 Berkeley Tech. L.J. 117-182.
- Perry W. L. et al. 2013. Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations (Santa Monica : RAND Corporation). https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.
- Robinson D., Yu H., Rieke A. 2014. *Civil Rights, Big Data, and Our Algorithmic Future. A September 2014 report on social justice and technology*.

https://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf.

- The White House, Executive Office of the President. 2016. *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*. *https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.*
- The White House, Executive Office of the President. 2014. *Big Data: Seizing Opportunities, Preserving Values.* *https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf*.
- Vedder, A.H. 1997. Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations. In Moore, G. (ed). Business Ethics: Principles and Practice (Business Education Publishers).